JunosE™ Software for E Series™ Broadband Services Routers

L2TP LAC

Release
14.3.x

Published: 2013-07-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

JunosE™ Software for E Series™ Broadband Services Routers L2TP LAC
Release 14.3.x

Revision History
July 2013—FRS JunosE 14.3.x

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

E Series and JunosE Documentation and Release Notes

For a list of related JunosE documentation, see http://www.juniper.net/techpubs/software/index.html.

If the information in the latest release notes differs from the information in the documentation, follow the *JunosE Release Notes.*

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JunosE Text and Syntax Conventions

Table 1 on page xiv defines notice icons used in this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xiv defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	• Issue the **clock source** command. • Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	**host1(config)#traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	**host1#show ip ospf 2**
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	• Emphasizes words. • Identifies variables. • Identifies chapter, appendix, and book names.	• There are two levels of access: *user* and *privileged*. • *clusterId, ipAddress.* • *Appendix A, System Specifications*
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic | line
[ ] (brackets)	Represent optional keywords or variables.	[internal | external]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at http://www.juniper.net/.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

http://www.juniper.net/techpubs/resources/index.html

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site athttp://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

L2TP Functionalities

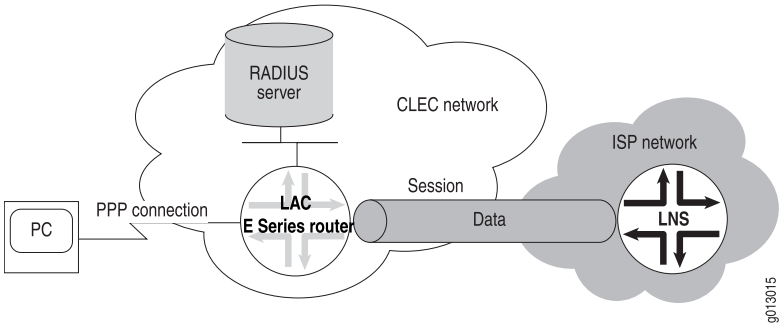
L2TP Overview

L2TP encapsulates layer 2 packets, such as PPP, for transmission across a network. An L2TP access concentrator (LAC), configured on an access device, such as an E Series router, receives packets from a remote client and forwards them to an L2TP network server (LNS), on a remote network.

You can configure your router to act as an LAC in pass-through mode in which the LAC receives packets from a remote client and then forwards them at layer 2 directly to the LNS.

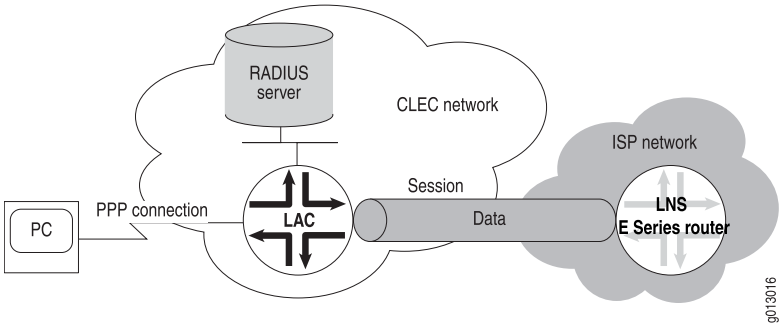
The E Series router creates tunnels dynamically by using authentication, authorization, and accounting (AAA) authentication parameters and transmits L2TP packets to the LNS via IP/User Datagram Protocol (UDP). Traffic travels in an L2TP *session*. A tunnel is an aggregation of one or more sessions. Figure 1 on page 3 and Figure 2 on page 4 show the E Series router in typical LAC and LNS arrangements.

Figure 1: Using the E Series Router as an LAC



.

Figure 2: Using the E Series Router as an LNS



NOTE: The E Series router does not support terminating both ends of a tunnel or session in the same router.

Related Documentation

- Implementing L2TP on page 7
- L2TP Platform Considerations on page 10
- L2TP References on page 11

L2TP Terminology

Table 3 on page 4 describes the basic terms for L2TP.

Table 3: L2TP Terms

Term	Description
Attribute value pair (AVP)	Combination of a unique attribute—represented by an integer—and a value containing the actual value identified by the attribute.
LAC	L2TP access concentrator (LAC)—a node that acts as one side of an L2TP tunnel endpoint and is a peer to the LNS. An LAC sits between an LNS and a remote system and forwards packets to and from each.
Call	A connection (or attempted connection) between a remote system and an LAC.
LNS	L2TP network server (LNS)—a node that acts as one side of an L2TP tunnel endpoint and is a peer to the LAC. An LNS is the logical termination point of a PPP connection that is being tunneled from the remote system by the LAC.
Peer	In the L2TP context, refers to either the LAC or LNS. An LAC's peer is an LNS, and vice versa.
Proxy authentication	Authentication data from the PPP client that is sent from the LNS as part of a proxy LCP. Data might include attributes such as authentication type, authentication name, and authentication challenge.

Table 3: L2TP Terms *(continued)*

Term	Description
Proxy LCP	LCP (Link Control Protocol) negotiation that is performed by the LAC on behalf of the LNS. Proxy sent by the LAC to the LNS containing attributes such as the last configuration attributes sent and received from the client.
Remote system	An end-system or router attached to a remote access network, which is either the initiator or recipient of a call.
Session	A logical connection created between the LAC and the LNS when an end-to-end PPP connection is established between a remote system and the LNS. **NOTE:** There is a one-to-one relationship between established L2TP sessions and their associated PPP connections.
Tunnel	A connection between an LAC-LNS pair consisting of a control connection and 0 or more L2TP sessions.

Related Documentation

- L2TP Overview on page 3

Packet Fragmentation

The E Series router supports the reassembly of IP-fragmented L2TP packets. (For more information, see the *IP Reassembly for Tunnels* chapter in *JunosE IP Services Configuration Guide*.) However, it is preferable to prevent fragmentation within L2TP tunnels because of the effects of fragmentation and reassembly on performance.

To prevent fragmentation, PPP LCP negotiation of the maximum receive unit (MRU) may be used to determine a proper maximum transmission unit (MTU). However, the normal automatic method of determining the proper MRU to negotiate (by evaluating the MRU of all lower layers in the interface stack) is not adequate for L2TP. The initial LCP negotiation between PPP in the client and the LAC is inadequate because it does not cover the entire extent of the eventual PPP session that travels all the way from the client to the LNS. Furthermore, even if PPP in the LNS chooses to renegotiate the MRU, it has no way to determine the proper MRU, since it does not know the minimum MRU on all of the intervening links between it and the LAC.

To overcome the inadequacy of normal determination of the MRU under such circumstances, you can configure the PPP MRU size by using the **ppp mru** command in Profile Configuration mode, Interface Configuration mode, or Subinterface Configuration mode. Use Profile Configuration mode for dynamic PPP interfaces, and Interface Configuration mode or Subinterface Configuration mode for static PPP interfaces.

When you specify the size, you need to take into account the MRU for all possible links between the LAC and the LNS. You must also take into account the L2TP encapsulation that is added to all packets entering the tunnel.

For example, if the link between the LAC and LNS with the lowest MRU were an Ethernet link, the following calculation applies:

Minimum link MRU	1500
L2TP encapsulating IP header	-20
L2TP encapsulating UDP header	-8
Maximum L2TP header (assumes a maximum of 16 bytes of Offset Pad)	-30
MRU size to specify	1442

If the smallest intervening link is an Ethernet link, specifying **ppp mru 1442** at either the LAC or LNS guarantees that no fragmentation will occur within the L2TP tunnel.

Related Documentation

- L2TP Overview on page 3
- Implementing L2TP on page 7

CHAPTER 2

L2TP Deployment

Implementing L2TP

The implementation of L2TP for the E Series router uses four levels:

- System—The router
- Destination—The remote L2TP system
- Tunnel—A direct path between the LAC and the LNS
- Session—A PPP connection in a tunnel

When the router has established destinations, tunnels, and sessions, you can control the L2TP traffic. Making a change to a destination affects all tunnels and sessions to that destination; making a change to a tunnel affects all sessions in that tunnel. For example, closing a destination closes all tunnels and sessions to that destination.

Sequence of Events on the LAC

The E Series router creates destinations, tunnels, and sessions dynamically, as follows:

1. The client initiates a PPP connection with the router.
2. The router and the client exchange Link Control Protocol (LCP) packets. For details about negotiating PPP connections, see the *Configuring Point-to-Point Protocol* chapter in *JunosE Link Layer Configuration Guide*.
3. By using either a local database related to the domain name or RADIUS authentication, the router determines either to terminate or to tunnel the PPP connection.
4. If the router discovers that it should tunnel the session, it does the following:
   a. Sets up a new destination or selects an existing destination.
   b. Sets up a new tunnel or selects an existing tunnel.
   c. Opens a new session.
5. The router forwards the results of the LCP negotiations and authentication to the LNS.

A PPP connection now exists between the client and the LNS.

NOTE: The router discards received packets if the size of the variable-length, optional offset pad field in the L2TP header is too large. The router always supports packets that have an offset pad field of up to 16 bytes, and may support larger offset pad fields, depending on other information in the header. This restriction is a possible, although unlikely, cause of excessive discarding of L2TP packets.

Sequence of Events on the LNS

The E Series router sets up an LNS as follows:

1. An LAC initiates a tunnel with the router.
2. The router verifies that a tunnel with this LAC is valid—destination configured, hostname and tunnel password correct.
3. The router completes the tunnel setup with the LAC.
4. The LAC sets up a session with the router.
5. The router creates a dynamic PPP interface on top of the session.
6. If they are enabled and present, the router takes the proxy LCP and the proxy authentication data and passes them to PPP.
7. The E Series PPP processes the proxy LCP, if it is present, and, if acceptable, places LCP on the router in opened state without renegotiation of LCP.

   NOTE: If proxy LCP is not present or not acceptable, the router negotiates LCP with the remote system.

8. The E Series PPP processes the proxy authentication data, if it is present, and passes the data to AAA for verification. (If the data is not present, E Series PPP requests the data from the remote system.)
9. The router passes the authentication results to the remote system.

Related Documentation

- L2TP Overview on page 3
- L2TP Platform Considerations on page 10
- L2TP Module Requirements on page 9
- L2TP References on page 11

CHAPTER 3

L2TP Platform and Module Requirements

L2TP Module Requirements

The supported modules for LNS depends on the type of E Series router that you have.

ERX7xx Models, ERX14xx Models, and the ERX310 Router

To use an LNS on ERX7xx models, ERX14xx models, and the ERX310 router, at least one Service line module (SM) or a module that supports the use of shared tunnel-server ports must be installed in the ERX router. For information about installing modules in the ERX router, see the *ERX Hardware Guide*.

SMs provide dedicated tunnel-server ports that are always configured on the module. Unlike other line modules, SMs do not pair with corresponding I/O modules that contain ingress and egress ports. Instead, they receive data from and transmit data to other line modules with access to ingress and egress ports on their own associated I/O modules.

You can also create tunnels on E Series modules that support shared tunnel-server ports. You can configure (provision) a shared tunnel-server port to use a portion of the module's bandwidth to provide tunnel services. For a list of the modules that support shared tunnel-server ports, see the *ERX Module Guide*.

When you configure the GE-2 line module or the GE-HDE line module with a shared tunnel-server port, the available bandwidth for tunnel services is limited to 0.5 Gbps per module. When you configure the ES2 4G line module with a shared tunnel-server port, the available bandwidth for tunnel services is limited to 0.8 Gbps per module.

For information about configuring tunnel services on dedicated and shared tunnel-server ports, see the *Managing Tunnel-Service and IPsec-Service Interfaces* chapter in *JunosE Physical Layer Configuration Guide*.

For information about line modules supported by the LAC and LNS and the type of support each module type receives, see *ERX Module Guide, Appendix A, Module Protocol Support*.

E120 Router and E320 Router

To use an LNS on an E120 router or an E320 router, you must install an ES2 4G line module (LM) or an ES2 10G ADV LM with an ES2-S1 Service I/O adapter (IOA). With the ES2 4G LM, it is also possible to use an LNS with an IOA that supports the use of shared tunnel-server ports. For information about installing modules in these routers, see the *E120 and E320 Hardware Guide*.

The combination of an ES2 4G LM or an ES2 10G ADV LM with an ES2-S1 Service IOA provides a dedicated tunnel-server port that is always configured on the IOA. Unlike SMs, the ES2 4G LM and the ES2 require the ES2-S1 Service IOA to condition it to receive and transmit data to other line modules. The ES2-S1 Service IOA also does not have ingress or egress ports. The ES2 10G ADV LM with the ES2-S1 Service IOA supports L2TP LNS functionality, which supports IPv4 as well as IPv6 encapsulated within PPP and L2TP over IPv4.

You can also create tunnels on IOAs that support shared tunnel-server ports. You can configure (provision) a shared tunnel-server port to use a portion of the bandwidth of the IOA to provide tunnel services. For a list of the IOAs that support shared tunnel-server ports, see the *E120 and E320 Module Guide*.

For information about IOAs that are supported by the LAC and LNS and the type of support each module type receives, see *E120 and E320 Module Guide, Appendix A, IOA Protocol Support*.

Related Documentation

- L2TP Overview on page 3
- Implementing L2TP on page 7
- L2TP Platform Considerations on page 10
- L2TP References on page 11

L2TP Platform Considerations

For information about modules that support LNS and LAC on the ERX7xx models, ERX14xx models, and the ERX310 Broadband Services Router:

- See *ERX Module Guide, Table 1, ERX Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support LNS and LAC.

For information about modules that support LNS and LAC on the E120 and E320 Broadband Services Routers:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support LNS and LAC.

Related Documentation

- L2TP Overview on page 3
- L2TP References on page 11

L2TP References

For more information about L2TP, see the following resources:

- RFC 2661—Layer Two Tunneling Protocol " L2TP" (August 1999)
- RFC 3145—L2TP Disconnect Cause Information (July 2001)
- Fail Over extensions for L2TP " failover" —draft-ietf-l2tpext-failover-06.txt (April 2006 expiration)
- RFC 4951—Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover" (August 2007)

For information about L2TP high availability support, see the *Managing High Availability* chapter in *JunosE System Basics Configuration Guide*.

For information about setting up policy-based routing features for L2TP, such as rate limit profiles, classifier control lists, and policy lists, see the *JunosE Policy Management Configuration Guide*.

For information about creating and attaching QoS profiles to L2TP sessions, see the *JunosE Quality of Service Configuration Guide*.

For information about how to secure Layer 2 Tunneling Protocol (L2TP) tunnels with IP Security (IPsec) on your E Series router, see the *Securing L2TP and IP Tunnels with IPsec* chapter in *JunosE IP Services Configuration Guide*.

Related Documentation

- L2TP Overview on page 3
- L2TP Platform Considerations on page 10

CHAPTER 4

L2TP Sessions and Tunnels

Sessions and Tunnels Supported

The E120 and E320 routers support 60,000 L2TP sessions, the ERX1440 router supports 32,000 L2TP sessions, and all other E Series routers support a maximum of 16,000 L2TP sessions. The following guidelines apply:

- On all E Series routers

  The SM and the ES2-S1 Service IOA both support the termination of 16,000 LNS sessions per module. Therefore, if you want to apply input or output policies to all of the available LNS sessions, you can only terminate a maximum of 8000 sessions per module.

- On the E120 router, E320 router, and the ERX1440 router

  You can create a systemwide maximum of 60,000 sessions per E120 or E320 router or 32,000 sessions per ERX1440 router. The maximum session limit is spread in any combination across a maximum of 8000 tunnels. For a router that is operating as an LAC for some tunnels and as an LNS for others, the 8000 tunnels and the router's applicable maximum sessions limits apply to the combined total of LAC and LNS tunnels and sessions.

- On all E Series routers except the ERX1440 router, E120 router, and the E320 router

  You can create a systemwide maximum of 16,000 sessions spread in any combination across a maximum of 8000 tunnels shared between an LAC and an LNS. For a router that is operating as an LAC for some tunnels and as an LNS for others, the 8000 tunnels and 16,000 sessions limits apply to the combined total of LAC and LNS tunnels and sessions.

NOTE: In previous releases, the JunosE Software required that you use the **license l2tp-session** command to configure a license to enable support for the maximum allowable L2TP sessions on ERX1440 routers, E120 routers, and E320 routers. The **license l2tp-session** command still appears in the CLI, but it has no effect on the actual enforced limit. The reported license limit is 60,000. The **show license l2tp-session** command also still appears in the CLI.

- To obtain the maximum number of ingress and egress policy attachments supported for L2TP sessions, see *JunosE Release Notes, Appendix A, System Maximums*.

Related Documentation

- L2TP Overview on page 3
- Implementing L2TP on page 7
- L2TP Module Requirements on page 9

Stateful Line Module Switchover Platform Considerations

Stateful line module switchover is supported on all E120 and E320 routers that contain ES2 4G line modules installed with the ES2-ES1 Service IOA. See the *E120 and E320 Module Guide* for modules supported on the E120 and E320 Broadband Services Routers.

Table 4 on page 14 lists the line module, SRP module, and IOA slot combinations that support stateful switchover of line modules and stateful switchover for LNS sessions, when the router operates as an LNS device on one side of an L2TP tunnel.

Table 4: Module Configurations Supported for Stateful Switchover of LNS Sessions

Router Model	SRP and SFM Model	Number of L2TP tunnels and sessions	Number of Active and Standby ES2-ES1 Service IOAs	Downlink and Uplink LMs	Support for Stateful Switchover of LNS Sessions
E320	SRP-100	16,000 tunnels and 16,000 sessions	2 Service IOAs (1 active and 1 standby)	ES2 4G LM and GE-4 IOA	Supported
E320	SRP-100	16,000 tunnels and 32,000 sessions	4 Service IOAs (2 active and 2 standby)	ES2 4G LM and GE-4 IOA	Supported
E320	SRP-320	32,000 tunnels and 32,000 sessions	4 Service IOAs (2 active and 2 standby)	ES2 4G LM and GE-4 IOA	Supported
E120	SRP-320	16,000 tunnels and 16,000 sessions	2 Service IOAs (1 active and 1 standby)	ES2 10G LM and GE-8 IOA	Not supported
E120	SRP-320	32,000 tunnels and 32,000 sessions	4 Service IOAs (2 active and 2 standby)	ES2 10G LM and GE-8 IOA	Not supported

Table 4: Module Configurations Supported for Stateful Switchover of LNS Sessions *(continued)*

Router Model	SRP and SFM Model	Number of L2TP tunnels and sessions	Number of Active and Standby ES2-ES1 Service IOAs	Downlink and Uplink LMs	Support for Stateful Switchover of LNS Sessions
E120	SRP-320	16,000 tunnels and 16,000 sessions	2 Service IOAs (1 active and 1 standby)	ES2 4G LM and GE-8 IOA	Supported
E120	SRP-320	32,000 tunnels and 32,000 sessions	4 Service IOAs (2 active and 2 standby)	ES2 4G LM and GE-8 IOA	Supported

Related Documentation

- *Stateful Line Module Switchover Overview*
- *System Operations When Stateful Line Module Switchover Is Enabled*
- *Replacement of Line Modules When Stateful Line Module Switchover Is Enabled*
- *Application Support for Stateful Line Module Switchover*

CHAPTER 5

Methods of Mapping a User Domain to an L2TP Tunnel

Mapping a User Domain Name to an L2TP Tunnel Overview

The router uses either the local database related to the domain name or a RADIUS server to determine whether to terminate or tunnel PPP connections.

For information about setting up RADIUS to provide this mapping, see the *Configuring Remote Access* chapter.

For a given domain map, you can choose one of two methods to map the domain to an L2TP tunnel locally on the router:

- Configure tunnels for a domain map and then define tunnel attributes from Domain Map Tunnel configuration mode.
- Configure a tunnel group and then define the attributes for its tunnels from Tunnel Group Tunnel Configuration mode. Use this method only when no tunnels are currently defined for the domain map from Domain Map Tunnel configuration mode. By default, tunnel groups are not assigned to the domain map.

  After configuring a tunnel group and the attributes for its tunnels, you can assign the tunnel group to the domain map from Domain Map mode. The tunnel group reference in the domain map is used instead of tunnel definitions configured from Domain Map Tunnel configuration mode.

  The RADIUS server can reference tunnel groups through the RADIUS Tunnel Group [26-64] attribute. The advantages of RADIUS support for tunnel groups are:

  - The RADIUS server can maintain a single tunnel group attribute associated with each user instead of sets of tunnel attributes for each user.
  - The RADIUS server can authenticate users before attempting to establish tunnels.

You can configure up to 31 tunnel definitions for an L2TP subscriber using either AAA domain maps or RADIUS returned values. Each tunnel definition contains both fixed-length and variable-length tunnel attributes. All tunnel definitions and their attributes that are stored in AAA are mirrored in a single transaction. When the size of the mirrored storage

transaction exceeds 9866 bytes, the router disables stateful SRP switchover (high availability).

The size of the transaction can exceed 9866 bytes when you configure all the variable length tunnel attributes of more than 17 tagged tunnel definitions, using either RADIUS or domain maps, to their maximum values. When the size of a transaction exceeds 9866 bytes, the router now mirrors the tunnel definitions in a different transaction. As a result, stateful SRP switchover is not disabled when you configure all the variable length tunnel attributes of all 31 tunnel definitions to their maximum values or when the RADIUS server sends tunnel attributes whose length exceeds the maximum length.

Related Documentation

- Mapping User Domain Names to L2TP Tunnels from Domain Map Tunnel Mode on page 44
- Mapping User Domain Names to L2TP Tunnels from Tunnel Group Tunnel Mode on page 48

CHAPTER 6

Termination of PPP and L2TP Subscriber Sessions

VSAs for Dynamic IP Interfaces Overview

Table 5 on page 19 describes the VSAs that apply to dynamic IP interfaces and are supported on a per-user basis from RADIUS. For details, see *JunosE Link Layer Configuration Guide*.

Table 5: VSAs That Apply to Dynamic IP Interfaces

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Ingress-Policy-Name	Specifies the name of the input (ingress) policy	26	len	10	sublen	string: *input-policy-name*
Egress-Policy-Name	Specifies the name of the output (egress) policy	26	len	11	sublen	string: *output-policy-name*
Ingress-Statistics	Indicates whether statistics are collected on input	26	12	12	6	integer: 0 – disable, 1 – enable
Egress-Statistics	Indicates whether statistics are collected on output	26	12	13	6	integer: 0 – disable, 1 – enable

Table 5: VSAs That Apply to Dynamic IP Interfaces *(continued)*

VSA	Description	Type	Length	Subtype	Subtype Length	Value
QoS-Profile-Name	Specifies the name of the QoS profile to attach to the interface	26	len	26	sublen	string: *qos-profile-name*

To use the VSAs shown in Table 5 on page 19:

- Specify the policy, or one or more QoS VSAs in the desired RADIUS user entries.
- Create the ingress or egress policy, or the QoS profile. Policies minimally consist of one or more policy commands and may include classifier control lists and rate limit profiles. See the *JunosE Policy Management Configuration Guide* for more information about policies and policy routing. See the *JunosE Quality of Service Configuration Guide* for information about creating QoS profiles.

When a dynamic interface is created according to a profile, the router checks with RADIUS to determine whether an input or output policy or a QoS profile must be applied to the interface. The VSA, if present, provides the name, enabling policy or QoS profile lookup. If found, the policy or QoS profile is applied to the dynamic interface.

The router also determines whether the creation profile specifies any policies to be applied to the interface. Policies specified by the RADIUS VSA supersede any specified by the profile, as described in the following example:

The RADIUS user entry includes an Ingress-Policy-Name VSA that specifies the policy input5. The profile specifies two policies, input7 and output1. In this case, the RADIUS-specified input policy (input5) and the profile-specified output policy (output1) are applied to the dynamic interface.

For information about assigning policies via profiles, see the *JunosE Policy Management Configuration Guide*. Only attributes assigned by RADIUS appear in RADIUS Acct-Start messages. RADIUS attributes specified by a profile for dynamic interfaces do not appear in RADIUS Acct-Start messages because the profile is not active when the Acct-Start message is generated. These attributes appear in RADIUS Acct-Stop messages for a profile that is active when the session is terminated.

The following section explains traffic shaping for PPP over ATM interfaces:

- Traffic Shaping for PPP over ATM Interfaces on page 20

Traffic Shaping for PPP over ATM Interfaces

The router supports the configuration of traffic shaping parameters for PPP over ATM (PPPoA) via domain-based profiles and RADIUS. In connection with this feature, Table 6 on page 21 describes VSAs that apply to dynamic IP interfaces and are supported on a per-user basis from RADIUS.

Table 6: Traffic-Shaping VSAs That Apply to Dynamic IP Interfaces

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Service-Category	Specifies the type of service	26	12	14	6	integer: 1 – UBR 2 – UBR PCR 3 – NRT VBR 4 – CBR 5 – RT VBR
PCR	Specifies the value for the peak cell rate (PCR)	26	12	15	6	integer
SCR	Specifies the value for the sustained cell rate (SCR)	26	12	16	6	integer
MBS	Specifies the maximum burst size (MBS)	26	12	17	6	integer

To configure traffic-shaping parameters for PPPoA via domain maps, use the **atm** command in Domain Map Configuration mode.

Related Documentation

- *Creating an IP Interface*

Mapping Application Terminate Reasons and RADIUS Terminate Codes Overview

The JunosE Software uses a default configuration that maps terminate reasons to RADIUS Acct-Terminate-Cause attributes. You can optionally create customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute—these mappings enable you to provide different information about the cause of a termination.

When a subscriber's L2TP or PPP session is terminated, the router logs a message for the internal terminate reason and logs another message for the RADIUS Acct-Terminate-Cause attribute (RADIUS attribute 49). RADIUS attribute 49 is also included in RADIUS Acct-Off and Acct-Stop messages. You can use the logged information to help monitor and troubleshoot terminated sessions.

Use the **show terminate-code** command to display information about the mappings between application terminate reasons and RADIUS Acct-Terminate-Cause attributes.

Table 7 on page 22 lists the IETF RADIUS Acct-Terminate-Cause codes that you can use to map application terminate reasons. In addition, you can also configure and use proprietary codes for values beyond 22.

Table 7: Supported RADIUS Acct-Terminate-Cause Codes

Code	Name	Description
1	User Request	User initiated the disconnect (log out)
2	Lost Carrier	DCD was dropped on the port
3	Lost Service	Service can no longer be provided; for example, the user's connection to a host was interrupted
4	Idle Timeout	Idle timer expired
5	Session Timeout	Subscriber reached the maximum continuous time allowed for the service or session
6	Admin Reset	System administrator reset the port or session
7	Admin Reboot	System administrator terminated the session on the NAS; for example, prior to rebooting the NAS
8	Port Error	NAS detected an error on the port that required ending the session
9	NAS Error	NAS detected an error (other than on the port) that required ending the session
10	NAS Request	NAS ended the session for a non-error reason
11	NAS Reboot	NAS ended the session due to a non-administrative reboot
12	Port Unneeded	NAS ended the session because the resource usage fell below the low threshold; for example, the bandwidth-on-demand algorithm determined that the port was no longer needed
13	Port Preempted	NAS ended the session to allocate the port to a higher-priority use
14	Port Suspended	NAS ended the session to suspend a virtual session
15	Service Unavailable	NAS was unable to provide the requested service
16	Callback	NAS is terminating the current session in order to perform callback for a new session
17	User Error	An error in the user input caused the session to be terminated
18	Host Request	The login host terminated the session normally
19	Supplicant Restart	Supplicant state machine was reinitialized
20	Reauthentication Failure	A previously authenticated supplicant failed to reauthenticate successfully following expiration of the reauthentication timer or explicit reauthentication request by management action

Table 7: Supported RADIUS Acct-Terminate-Cause Codes *(continued)*

Code	Name	Description
21	Port Reinitialized	The port's MAC has been reinitialized
22	Port Administratively Disabled	The port has been administratively disabled

Related Documentation

- *Configuring Custom Mappings for PPP Terminate Reasons*

CHAPTER 7

How L2TP Dial-Out Works

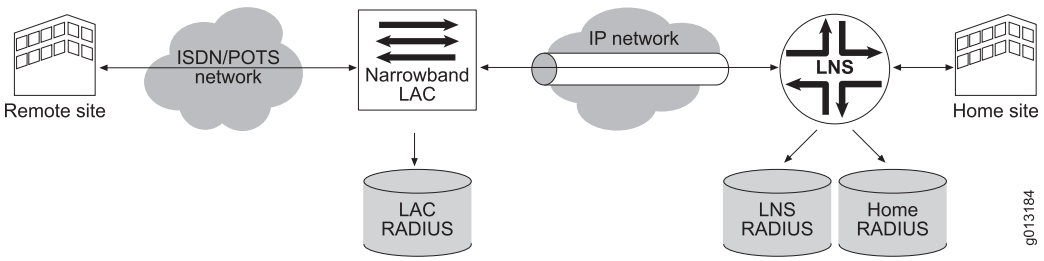
L2TP Dial-Out Overview

L2TP dial-out provides a way for corporate virtual private networks (VPNs) that use Broadband Remote Access Server (B-RAS) to dial out to remote offices that have only narrowband dial-up access. The L2TP network server (LNS) function is deployed in networks that have a combination of broadband and narrowband access.

A remote site can communicate on demand with the home site with a normal L2TP access concentrator (LAC) to LNS session. When the communication finishes, the remote site terminates the session. However, if the home site wishes to communicate with the remote site and no incoming call is currently established, the home site needs a method to dial out to the remote site. This method is L2TP dial-out, which uses the L2TP outgoing call support defined in RFC 2661—Layer Two Tunneling Protocol " L2TP" (August 1999).

Figure 3 on page 25 shows the dial-out model in which the LNS initiates L2TP sessions and provides enough information to the narrowband LAC so that it can complete the dial-out from the home site to the remote site.

Figure 3: Network Model for Dial-Out



NOTE: The dial-out feature exists in the LNS only. It does not exist in the LAC.

Related Documentation

- L2TP Overview on page 3
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Network Model on page 26
- L2TP Dial-Out Operational States on page 28
- L2TP Dial-Out Process on page 27
- L2TP Dial-Out Outgoing Call Setup Details on page 31

L2TP Dial-Out Platform Considerations

L2TP dial-out is supported on all E Series routers.

For information about the modules supported on E Series routers:

- See the *ERX Module Guide* for modules supported on ERX7xx models, ERX14xx models, and the ERX310 Broadband Services Router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 and E320 Broadband Services Routers.

Related Documentation

- L2TP Dial-Out Overview on page 25
- L2TP Dial-Out Network Model on page 26

L2TP Dial-Out References

For more information about L2TP, see RFC 2661—Layer Two Tunneling Protocol " L2TP" (August 1999).

Related Documentation

- L2TP Dial-Out Overview on page 25
- L2TP Dial-Out Network Model on page 26

L2TP Dial-Out Network Model

In the figure in "L2TP Dial-Out Overview" on page 25, the home site connects to the Internet over a permanent leased line to the Internet service provider's (ISP's) E Series LNS. The ISP uses an IP network to connect the LNS to the narrowband access point of the network where the narrowband LAC exists. The narrowband LAC connects to a narrowband network (ISDN) that the remote site is also connected to.

The figure shows three RADIUS servers. The home site maintains the home server, and the other two servers are at the LNS and the LAC. The router accesses the home and LNS RADIUS servers. (The separation of the RADIUS servers is transparent to the router.)

Before any attempts at connectivity can take place from the home site to the remote site, an administrator must configure a dial-out route on the router. This route directs the router to start a dial-out operation. The route includes a dial-out target (the virtual router context and the IP address of the remote site). When the router receives a packet destined for the target, it triggers a dial-out session to the target. The route is associated with a profile that holds parameters for the interface stack that the router builds as a result of the dial-out.

Related Documentation

- L2TP Dial-Out Overview on page 25
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Operational States on page 28
- L2TP Dial-Out Process on page 27
- L2TP Dial-Out Outgoing Call Setup Details on page 31

L2TP Dial-Out Process

The following is the dial-out process used in the network model illustrated in "L2TP Dial-Out Overview" on page 25:

1. The router receives a trigger packet.
2. The router builds a RADIUS Access-Request message and sends it to the RADIUS server that is associated with the virtual router on which the dial-out route is defined—typically, the RADIUS home server.
3. The RADIUS server's response to the Access-Request is similar to the response used for LAC incoming calls. Notable differences are that the IP addresses of the peer are interpreted as LAC addresses instead of LNS addresses. In addition, narrowband details, such as calling numbers, are returned.
4. The LNS makes the outgoing call using a load-balancing or round-robin mechanism identical to the one that the E Series LAC uses for incoming calls. The LAC may also employ the LAC RADIUS in tunnel authentication.
5. Once the LNS successfully completes a control connection and session with the LAC, the LAC performs the actual narrowband dial-out operation to the remote site using the information passed by the LNS during session setup.
6. A PPP session is started on the remote customer premises equipment (CPE), and mutual PPP authentication is performed at the remote CPE and the LNS as follows:
   a. The LNS uses the LNS RADIUS server to validate the remote CPE's PPP session, while the CPE can use its own RADIUS server to validate the LNS's PPP session.
   b. The LNS uses the username and password that is returned in the first Access-Accept message.
7. Once authentication is successful, an IP interface is built on top of the PPP interface at the LNS. Internet Protocol Control Protocol (IPCP) is negotiated, and the framed route that RADIUS returns as a result of the PPP authentication supersedes the dial-out route.

IP traffic can now flow freely between the home and remote sites.

Related Documentation

- L2TP Dial-Out Overview on page 25
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Network Model on page 26
- L2TP Dial-Out Operational States on page 28
- L2TP Dial-Out Outgoing Call Setup Details on page 31

L2TP Dial-Out Operational States

The dial-out state machine is a control process within the router that manages the dial-out function for each IP flow. The dial-out state machine has four levels of control: the router chassis, virtual router, targets, and sessions. This section describes the operational states of each of these levels.

Chassis

Table 8 on page 28 describes the operational states of the chassis.

Table 8: Chassis Operational States

State	Description
inService	Dial-out service is operational at the chassis level.
initializationFailed	Dial-out service could not obtain enough system resources for basic operation. All configuration commands fail, and the dial-out service does not function.

Virtual Router

Table 9 on page 28 describes the operational states of the virtual router.

Table 9: Virtual Router Operational States

State	Description
inService	Dial-out service is operational for the virtual router.
initPending	Dial-out service is waiting for the virtual router to be operational. Targets defined within the virtual router are not functional.
down	The dial-out interface for this virtual router is down. Targets defined within the virtual router are not functional.

Targets

Table 10 on page 29 describes the operational states of the targets.

Table 10: Target Operational States

State	Description
inService	Dial-out route is up and operational.
inhibited	Dial-out service cannot obtain sufficient resources to handle triggers, and all triggers are discarded. When resources become available, a target can transition from inhibited to inService. Note that sessions within an inhibited target that are already in the process of connecting or are in the inService state are not affected by this condition.
down	There are insufficient resources to support the creation of a dial-out route for the target. When resources become available, the target can transition to inService. Note that sessions within a down target that are already in the process of connecting or are in the inService state are not affected by this condition.

Sessions

Table 11 on page 29 describes operational states of the sessions.

Table 11: Session Operational States

State	Description
authenticating	New sessions start in the authenticating state. In this state, the dial-out state machine has received a valid trigger and is waiting for authentication, authorization, and accounting (AAA) to complete the initial authentication. On getting a grant from AAA, the session transitions to the connecting state. Alternatively, on getting a deny from AAA, the session transitions to the inhibited state.
connecting	Sessions enter the connecting state when authentication is complete. In this state, the dial-out state machine has initiated an outgoing L2TP call. On entering this state, the session-connecting timer is set to the chassis-wide trigger timer value. The session stays in this state until either the outgoing call is successful or the connecting timer expires. Any new trigger packets received for this session when it is in the connecting state are discarded.
inService	A session enters the inService state from the connecting state on successful completion of the dial-out call request. The session stays in this state until the outgoing call is closed.

Table 11: Session Operational States *(continued)*

State	Description
inhibited	A session enters the inhibited state from the connecting state when the connecting timer expires (that is, the outgoing call was unsuccessful). This state prevents the router from thrashing on an outgoing call that cannot be completed. When in this state, the router discards all trigger packets received for the session. The inhibited timer controls the amount of time spent in this state. The setting of the inhibited timer varies depending on whether the session is entering the inhibited state for the first time or is reentering the state. • If it is the first time, the inhibited timer is initialized to the chassis-wide trigger value. • If it is reentering the state, the inhibited timer is initialized to 2 times the previous value of the inhibited timer, up to a maximum of 8 times the chassis-wide trigger value. For example, if the chassis-wide trigger value is 30 seconds, the setting of the inhibited timer within the session (on subsequent immediate reentries; see postInhibited state) is 30, 60, 120, 240. Since 240 is 8 x 30, the inhibited timer for this session is never set larger than 240 seconds.
postInhibited	A session enters the postInhibited state after completion of an inhibited state. The inhibited timer is reused to control the amount of time the session stays in postInhibited state. In this state the timer repeatedly times out and reduces the inhibited timer by a factor of 2 on each iteration. Once the inhibited timer reaches zero, the session transitions to dormant. The receipt of a trigger in this state results in a transition to the authenticating state.
dormant	A session enters the dormant state after completion of a postInhibited state. The dormant timer is initialized to the chassis-wide dormant timer value, minus the time the session spent in the postInhibited state. Receipt of a new trigger packet transitions the session to the authenticating state. If the dormant timer expires, the session is deleted. The dormant state exists to allow analysis of a dial-out session before it is deleted.
pending	A session enters the pending state when a valid trigger is received but there already are the maximum number of connecting sessions in the router. The router discards all subsequent trigger packets until other sessions transition out of the connecting state. When this happens, pending sessions can transition to the dormant state.
failed	A session enters the failed state when the router detects a configuration error that prevents the successful operation of the session. Specifically, one of the final steps in a dial-out request is mutual PPP authentication at the LNS. A side-effect of authentication is the installation of an access route for the outgoing call. If the access route does not correspond to the trigger packet (that is, the trigger packet cannot be routed successfully by the new access route), the router detects this discrepancy as a configuration error because trigger packets that arrive are not forwarded into the outgoing call; rather, they are buffered or discarded. The only way to exit the failed state is with the **l2tp dial-out session reset** command.

Related Documentation

- L2TP Dial-Out Overview on page 25
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Network Model on page 26
- L2TP Dial-Out Process on page 27
- L2TP Dial-Out Outgoing Call Setup Details on page 31

L2TP Dial-Out Outgoing Call Setup Details

This section details the process described in "L2TP Dial-Out Process" on page 27.

Access-Request Message

To create the username in the authentication request, the router uses the trigger, dial-out route, domain name, and optional Multiprotocol Label Switching (MPLS) route distinguisher (RD). The username is constructed as follows:

[MPLS RD]/{trigger destination address}@domain-name

For example, given a dial-out route with an IP prefix of 10.10.0.0/16, a domain name of L2TP-dial-out.de.dt, and an MPLS RD of 0.0.0.0:65000, if a trigger packet arrives with a destination IP address of 10.10.1.1, the router creates the following username:

0.0.0.0:65000/10.10.1.1@L2TP-dial-out.de.dt

No password is offered, and the authentication request is passed to the S-series AAA server for normal authentication processing.

Using the above example, the AAA domain map processes the L2TP-dial-out.de.dt domain as for any other domain. If RADIUS authentication is configured for the authenticating virtual router (VR) context, AAA passes the authentication request to the E Series RADIUS client. The RADIUS authentication request is consistent with other requests, except that the Service-Type attribute is set to outbound (value of 5).

Access-Accept Message

The router expects RADIUS attributes that define a tunnel to be returned with the additions in Table 12 on page 31. If tunnel attributes are excluded from the Access-Accept message or the returned Service-Type attribute is not set to outbound, the dial-out session is denied.

Table 12: Additions to RADIUS Attributes in Access-Accept Messages

Attribute Number	Attribute Name	Content
6	Service-Type	Outbound
67	Tunnel-Server-Endpoint	IP address of LAC
Juniper VSA 26-35	Tunnel-Dialout-Number	L2TP dial-out number

Table 12: Additions to RADIUS Attributes in Access-Accept Messages *(continued)*

Attribute Number	Attribute Name	Content
Juniper VSA 26-36	PPP-Username	Username used in PPP L2TP dial-out sessions at the LNS
Juniper VSA 26-37	PPP-Password	Password used in PPP L2TP dial-out sessions at the LNS
Juniper VSA 26-38	PPP-Protocol	Authentication protocol used for L2TP sessions. 0 = none 1 = PAP 2 = CHAP 3 = PAP-CHAP 4 = CHAP-PAP
Juniper VSA 26-39	Tunnel-Min-Bps	Minimum line speed; passed to LAC (not interpreted by the LNS)
Juniper VSA 26-40	Tunnel-Max-Bps	Maximum line speed; passed to LAC (not interpreted by the LNS)
Juniper VSA 26-41	Tunnel-Bearer-Type	Bearer capability required: 0=name; 1=analog; 2=digital. Passed to LAC (not interpreted by the LNS).

Outgoing Call

After receiving a valid tunnel definition from AAA, the E Series LNS initiates an outgoing call. The router follows the same load-sharing mechanisms as for incoming calls. See "Configuring LAC Tunnel Selection Parameters" on page 51.

After an outgoing call is successfully signaled, the router dynamically creates a PPP interface. The profile in the dial-out route definition specifies any PPP configuration options. Both the L2TP session and the PPP interface exist on a Service module, identical to the LNS operation for incoming calls.

Once the PPP interface is created, Link Control Protocol (LCP) and IPCP are negotiated.

Mutual Authentication

Mutual authentication takes place in LCP, where the LNS validates the PPP interface on the remote CPE and vice-versa. LNS takes the same actions to authenticate the peer as it does on incoming calls.

The LNS obtains the PPP username and password from the initial Access-Accept message. It then provides this information to the remote CPE for authentication.

Route Installation

Once authentication is complete, the router creates a new access route. This route directs the forwarding of IP packets related to the original trigger packet to the newly created interface. The route does not need to be identical to the one specified in the dial-out route, but it must be able to forward packets that have the same destination address as the trigger packet. However, if the access route does not encompass the dial-out route definition, any other trigger packets initiate a new dial-out session.

The dial-out state machine verifies that the trigger packet can be forwarded over the route.

- If the verification is unsuccessful, the dial-out session is put into the failed state.
- If the verification is successful, the dial-out session is put into the inService state.

Related Documentation

- L2TP Dial-Out Overview on page 25
- *L2TP Dial-Out Terms*
- L2TP Dial-Out Network Model on page 26
- L2TP Dial-Out Operational States on page 28
- L2TP Dial-Out Process on page 27

PART 2

Configuration

CHAPTER 8

Configuring Settings for L2TP Destinations, Tunnels, and Sessions

Modifying L2TP LAC Default Settings for Managing Destinations, Tunnels, and Sessions

Configuring an E Series router for B-RAS enables the router to operate as an LAC with default settings. You can modify the default settings as follows:

- Enable the verification of data integrity via UDP.
- Specify the time period for which the router maintains dynamic destinations, tunnels, or sessions after termination.

NOTE: **The previous two operations also apply to an LNS, however there is no default configuration that enables the LNS.**

When the router is established as an LAC or LNS and is creating destinations, tunnels, and sessions, you can manage them as follows:

- Prevent the creation of new sessions, tunnels, and destinations.
- Close and reopen all or selected destinations, tunnels, and sessions.
- Configure drain timeout operations, which control the amount of time a disconnected LAC tunnel waits before restarting after receiving a restart request.
- Configure how many times the router retries a transmission if the initial attempt is unsuccessful.

NOTE: All the commands in this section apply to both the LAC and the LNS.

Related Documentation

- Generating UDP Checksums in Packets to L2TP Peers on page 38
- Specifying a Destruct Timeout for L2TP Tunnels and Sessions on page 38
- Preventing Creation of New Destinations, Tunnels, and Sessions on page 39
- Shutting Down Destinations, Tunnels, and Sessions on page 40
- Specifying the Number of Retransmission Attempts on page 42

Generating UDP Checksums in Packets to L2TP Peers

You can configure the router to generate a UDP data integrity checksum in data packets sent to an L2TP peer. The router always uses UDP checksums during transmission and reception of L2TP control packets. Generation of checksums is disabled by default.

- To enable generation of UDP checksums:

  ```
  host1(config)#l2tp checksum
  ```

NOTE: This command does not affect the way the router checks the UDP data integrity checksum in L2TP data packets that are received from an L2TP peer. The router checks all non-zero received checksums and discards the packet if a data integrity problem is detected.

L2TP checksum generation support is available on an ES2 10G Uplink LM and an ES2 4G LM only. It is not supported on an ES2 10G LM and an ES2 10G ADV LM. If an ES2 10G LM or an ES2 10G ADV LM is present when L2TP checksum is enabled, the checksum is not calculated and its value is set to zero.

Related Documentation

- l2tp checksum on page 93

Specifying a Destruct Timeout for L2TP Tunnels and Sessions

You can specify the maximum time period, in the range 10–3600 seconds (1 hour), for which the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed. The router uses a timeout of 600 seconds by default.

This command facilitates debugging and other analysis by saving underlying memory structures after the destination, tunnel, or session is terminated.

Any specific dynamic destination, tunnel, or session may not be maintained for this entire time period if the resources must be reclaimed early to allow new tunnels to be established.

When a subscriber is terminated, the server port that hosted the subscriber session is released after the dynamic interface destruct timeout is exceeded. The server port that is released is available for a new incoming-call request (ICRQ) packet that the LAC sends to the LNS. Until the time any server port is available to be used for a new incoming call, new ICRQ packets are denied because of a lack of system resources.

TIP: If you use the **l2tp destination lockout timeout** command to configure an optional lockout timeout, always configure the destruct timeout to be longer than the lockout timeout. The destruct timeout overrides the lockout timeout—when the destruct timeout expires, all information about the locked out destination is deleted, including the lockout timeout and lockout test settings. See *Managing the L2TP Destination Lockout Process*.

- To specify a destruct timeout:

  ```
  host1(config)#l2tp destruct-timeout 1200
  ```

Related Documentation

- l2tp destruct-timeout on page 94

Preventing Creation of New Destinations, Tunnels, and Sessions

You can configure several L2TP drain operations, which determine how the router creates new L2TP destinations, tunnels, and sessions. You can manage the following features:

1. Preventing Creation of New Destinations, Tunnels, and Sessions on the Router on page 39
2. Preventing Creation of New Tunnels and Sessions at a Destination on page 40
3. Preventing Creation of New Sessions for a Tunnel on page 40
4. Specifying a Drain Timeout for a Disconnected Tunnel on page 40

Preventing Creation of New Destinations, Tunnels, and Sessions on the Router

You use the **l2tp drain** command to prevent the creation of new destinations, tunnels, and sessions on the router.

The **l2tp drain** command and the **l2tp shutdown** command both affect the administrative state of L2TP on the router. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.

- To prevent the creation of new destinations, tunnels, and sessions:

  ```
  host1(config)#l2tp drain
  ```

Preventing Creation of New Tunnels and Sessions at a Destination

You use the **l2tp drain destination** command to prevent the creation of new tunnels and sessions at a specific destination.

The **l2tp drain destination** command and the **l2tp shutdown destination** command both affect the administrative state of L2TP for the destination. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.

- To prevent the creation of new tunnels and sessions at the specified destination:

  host1(config)#l2tp drain destination ip 172.31.1.98

Preventing Creation of New Sessions for a Tunnel

Use the **l2tp drain tunnel** command to prevent the creation of new sessions for a tunnel.

The **l2tp drain tunnel** command and the **l2tp shutdown tunnel** command both affect the administrative state of L2TP for the tunnel. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.

- To prevent the creation of new sessions for a specific tunnel:

  host1(config)#l2tp drain tunnel virtual-router default ip 172.31.1.98 isp.com

Specifying a Drain Timeout for a Disconnected Tunnel

Use the **l2tp tunnel short-drain-timeout** command to specify the amount of time a disconnected LAC L2TP tunnel waits before restarting after it receives a restart request.

You can specify a drain timeout in the range 0–31 seconds. This feature enables the router to restart tunnels more quickly than the standard 31-second drain time specified by RFC-2661. By default, the router uses a short-drain timeout of 2 seconds.

- To specify the short-drain timeout:

  host1(config)#l2tp tunnel short-drain-timeout 12

Shutting Down Destinations, Tunnels, and Sessions

You can configure how the router shuts down L2TP destinations, tunnels, and sessions. You can specify the following shutdown methods, which also prevent the creation of new tunnels:

1. Closing and Preventing Existing and New Destinations, Tunnels, and Sessions on the Router on page 41
2. Closing and Preventing Existing and New Tunnels and Sessions for a Destination on page 41

3. Closing and Preventing Existing and New Sessions in a Specific Tunnel on page 41
4. Closing a Specific Session on page 41

Closing and Preventing Existing and New Destinations, Tunnels, and Sessions on the Router

You use the **l2tp shutdown** command to close all existing destinations, tunnels, and sessions, and to prevent the creation of new destinations, tunnels, and sessions on the router.

If an SCCRQ message is received when the **l2tp shutdown** command is configured, then a StopCCN packet along with the appropriate Result Code AVP (Result Code value set to 2 and Error Code to 4) is sent to the LAC to indicate that the LNS is shut down.

The **l2tp shutdown** and **l2tp drain** commands affect the administrative state of L2TP on the router. Although each command has a different effect, the **no** version of each command leaves L2TP in the enabled state.

- To close all destinations, tunnels, and sessions on the router:

  host1(config)#l2tp shutdown

Closing and Preventing Existing and New Tunnels and Sessions for a Destination

You use the **l2tp shutdown destination** command to close all existing tunnels and sessions for a destination and to prevent the creation of tunnels and sessions for that destination.

The **l2tp shutdown destination** and **l2tp drain destination** commands affect the administrative state of L2TP for the destination. Although each command has a different effect, the **no** version of each command leaves L2TP in the enabled state.

- To close tunnels and sessions, and prevent the creation of new tunnels and sessions for the specified destination:

  host1(config)#l2tp shutdown destination 1

Closing and Preventing Existing and New Sessions in a Specific Tunnel

You use the **l2tp shutdown tunnel** command to close all sessions in a tunnel and to prevent the creation of sessions in a tunnel.

The **l2tp shutdown tunnel** command and the **l2tp drain tunnel** command both affect the administrative state of L2TP for the tunnel. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.

- To close all existing sessions in a specific tunnel and prevent creation of new sessions:

  host1(config)#l2tp shutdown tunnel 1/isp.com

Closing a Specific Session

You use the **l2tp shutdown session** command to close the specified session.

- To close a specific session:

  host1(config)#l2tp shutdown session 1/1/1

Specifying the Number of Retransmission Attempts

You can specify the number of retransmission attempts the router uses for tunnels, in the range 2–30. By default, the router uses a retry count of 5.

Use the **established** keyword to apply the retry count only to established tunnels. Use the **not-established** keyword to apply the retry count only to tunnels that are not established. If you do not include a keyword, the router applies the retry count to both established and nonestablished tunnels.

- To configure the number of retransmission attempts:

  host1(config)#l2tp retransmission 4 established

If you perform a stateful SRP switchover on an LNS device, we recommend that you configure the maximum number of retransmission attempts as 10, although the default number of attempts is 5. This recommendation applies for all types of L2TP peer resynchronization methods configured for LNS devices.

Related Documentation

- l2tp retransmission on page 102

CHAPTER 9

Configuring an L2TP LAC

LAC Configuration Prerequisites

Before you begin configuring the router as an LAC, perform the following steps:

1. Create a virtual router.

   host1(config)#virtual-router west

2. Assign a router ID IP address, such as that for a loopback interface, to the virtual router. This address must be reachable by the L2TP peer.

   host1:west(config)#ip router-id 10.10.45.3

   CAUTION: You must explicitly assign a router ID to a virtual router rather than using a dynamically assigned router ID. A fixed ID is required because every time the ID changes, L2TP must disconnect all existing tunnels and sessions that use the old ID. If you use a dynamically assigned router ID, the value can change without warning, leading to failure of all L2TP tunnels and sessions. Also, the router could dynamically assign a router ID that is not reachable by the L2TP peer, causing a complete failure of L2TP. You must set the router ID even if you specified a source address in the domain map or a local address in the host profile.

3. When configuring the router as a LAC, configure the router or virtual router for Broadband Remote Access Server (B-RAS).

NOTE: If you are using shared tunnel-server ports, you must configure the shared tunnel-server ports before you configure Layer 2 Tunneling Protocol (L2TP) network server (LNS) support. You use the **tunnel-server** command in Global Configuration mode to specify the physical location of the shared tunnel-server port that you want to configure.

See *JunosE Physical Layer Configuration Guide* for additional information about the **tunnel-server** command and shared tunnel-server ports.

Related Documentation

- virtual-router on page 133
- ip router-id on page 92

Mapping User Domain Names to L2TP Tunnels from Domain Map Tunnel Mode

To map a domain to an L2TP tunnel locally on the router from Domain Map Tunnel mode, perform the following steps:

1. Specify a domain name and enter Domain Map Configuration mode:

   ```
   host1(config)#aaa domain-map westford.com
   host1(config-domain-map)#
   ```

2. Specify a virtual router; in this case, the *default* router is specified.

   ```
   host1(config-domain-map)#router-name default
   ```

3. Specify a tunnel to configure and enter Domain Map Tunnel Configuration mode:

   ```
   host1(config-domain-map)#tunnel 3
   ```

4. Specify the LNS endpoint address of a tunnel.

   ```
   host1(config-domain-map-tunnel)#address 192.0.2.13
   ```

5. (Optional) Assign a tunnel group to the domain map. You can assign a tunnel group only when no tunnels are currently defined for the domain map from AAA Domain Map Tunnel mode.

   ```
   host1(config-domain-map)#tunnel group storm
   ```

6. Specify a preference for the tunnel.

   You can specify up to eight levels of preference, and you can assign the same preference to a maximum of 31 tunnels. When you define multiple preferences for a destination, you increase the probability of a successful connection.

   ```
   host1(config-domain-map-tunnel)#preference 5
   ```

7. (Optional) Specify an authentication password for the tunnel.

   ```
   host1(config-domain-map-tunnel)#password temporary
   ```

NOTE: If you specify a password for the LAC, the router requires that the peer (the LNS) authenticate itself to the router. In this case, if the peer fails to authenticate itself, the tunnel terminates.

8. (Optional) Specify a hostname for the LAC end of the tunnel.

   The LAC sends the hostname to the LNS when communicating to the LNS about the tunnel. The hostname can be up to 64 characters (no spaces).

   host1(config-domain-map-tunnel)#client-name host4

NOTE: If the LNS does not accept tunnels from unknown hosts, and if no hostname is specified, the LAC uses the router name as the hostname.

9. (Optional) Specify a server name for the LNS.

   This name specifies the hostname expected from the peer (the LNS) when you set up a tunnel. When this name is specified, the peer must identify itself with this name during tunnel startup. Otherwise, the tunnel is terminated. The server name can be up to 64 characters (no spaces).

   host1(config-domain-map-tunnel)#server-name boston

10. (Optional) Specify a source IP address for the LAC tunnel endpoint. All L2TP packets sent to the peer use this source address.

    host1(config-domain-map-tunnel)#source-address 192.0.3.3

    By default, the router uses the virtual router's router ID as the source address. You can override this behavior for an L2TP tunnel by specifying a source address. If you do specify a source address, use the address of a stable IP interface (for example, a loopback interface). Make sure that the address is configured in the virtual router for this domain map, and that the address is reachable by the peer.

11. Specify a tunnel identification. (The router groups L2TP sessions with the same tunnel identification into the same tunnel.)

    host1(config-domain-map-tunnel)#identification acton

    The router groups L2TP sessions with the same tunnel identification into the same tunnel. This occurs only when both the destination (virtual router, IP address) and the ID are the same.

12. Specify the L2TP tunnel type (RADIUS attribute 64, Tunnel-Type). Currently, the only supported value is L2TP.

    host1(config-domain-map-tunnel)#type l2tp

13. Specify a medium type for the tunnel. (L2TP supports only IP version 4 [IPv4].)

    host1(config-domain-map-tunnel)#medium ipv4

14. (Optional) Specify a default tunnel client name.

    host1(config-domain-map-tunnel)#exit

```
host1(config-domain-map)#exit
host1(config)#aaa tunnel client-name boxford
```

If the tunnel client name is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default name.

15. (Optional) Specify a default tunnel password.

```
host1(config)#aaa tunnel password 3&92k%b#q4
host1(config)#exit
```

If the tunnel password is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default password.

16. (Optional) Set the format for the tunnel assignment ID that is passed to PPP/L2TP.

The tunnel assignment ID format can be either only assignmentID or clientAuthId + serverAuthId + assignmentId.

```
host1(config)#aaa tunnel assignment-id-format assignmentID
```

If you do not set a tunnel assignment ID, the software sets it to the default (assignmentID). This parameter is only generated and used by the L2TP LAC device.

17. (Optional) Specify whether or not to use the tunnel peer's Nas-Port [5] and Nas-Port-Type [61] attributes.

When enabled, the attribute is supplied by the tunnel peer. When disabled, the attribute is not supplied. Use the **no** version of the command to restore the default, enable.

```
host1(config)#aaa tunnel ignore nas-port enable
host1(config)#aaa tunnel ignore nas-port-type disable
```

18. (Optional) Set up the router to ignore sequence numbers in data packets received on L2TP tunnels.

```
host1(config)#l2tp ignore-receive-data-sequencing
```

This command does not affect the insertion of sequence numbers in packets *sent* from the router.

BEST PRACTICE: We recommend that you set up the router to ignore sequence numbers in received data packets if you are using IP reassembly. Because IP reassembly might reorder L2TP packets, out-of-order packets might be dropped when sequence numbers are being used on L2TP data packets.

19. (Optional) Disable the generation of authentication challenges by the local tunnel, so that the tunnel does not send a challenge during negotiation. However, the tunnel does accept and respond to challenges it receives from the peer.

```
host1(config)#l2tp disable challenge
```

20. Verify the L2TP tunnel configuration.

```
host1(config)# show aaa domain-map
Domain: westford.com; router-name: default; ipv6-router-name: default
```

```
Tunnel
Tunnel   Tunnel         Tunnel        Tunnel   Tunnel    Tunnel    Tunnel
Client
 Tag      Peer          Source         Type    Medium   Password     Id
Name
------   ------------   -----------   ------   ------   ---------  ------
------
3        192.168.2.13   192.168.3.3   l2tp     ipv4     temporary  acton
host4
         Tunnel                 Tunnel                     Tunnel
Tunnel   Server     Tunnel       Max                        Virtual
 Tag      Name    Preference   Sessions     Tunnel RWS      Router
------   ------   ----------   --------   --------------   -------
3        boston   5            0          system chooses   vr2
```

```
host1#show aaa tunnel-parameters
Tunnel password is 3&92k%b#q4
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
Tunnel assignmentId format is assignmentId
Tunnel calling number format is descriptive
```

Related Documentation

- Mapping User Domain Names to L2TP Tunnels from Tunnel Group Tunnel Mode on page 48
- aaa domain-map on page 74
- aaa tunnel assignment-id-format on page 77
- aaa tunnel client-name on page 78
- aaa tunnel ignore on page 79
- aaa tunnel password on page 80
- address on page 84
- client-name on page 87
- identification on page 88
- l2tp disable challenge on page 97
- l2tp ignore-receive-data-sequencing on page 101
- medium ipv4 on page 112
- password on page 113
- preference on page 115
- router-name on page 125
- server-name on page 126
- source-address on page 128
- tunnel on page 129
- tunnel group on page 130

- type on page 131

Mapping User Domain Names to L2TP Tunnels from Tunnel Group Tunnel Mode

To map a domain to an L2TP tunnel locally on the router from Tunnel Group Tunnel Configuration mode, perform the following steps:

1. Specify an AAA tunnel group and change the mode to Tunnel Group Tunnel Configuration mode. From Tunnel Group Tunnel Configuration mode, you can add up to 31 tunnel definitions.

   host1(config)#aaa tunnel-group westford
   host1(config-tunnel-group)#

2. Specify a tunnel to configure and enter Tunnel Group Tunnel Configuration mode:

   host1(config-tunnel-group)#tunnel 3
   host1(config-tunnel-group-tunnel)#

3. Specify a virtual router; in this case, the *default* router is specified.

   host1(config-tunnel-group-tunnel)#router-name default

4. Specify the LNS endpoint address of a tunnel.

   host1(config-tunnel-group-tunnel)#address 192.0.2.13

5. Specify a preference for the tunnel.

   You can specify up to eight levels of preference, and you can assign the same preference to a maximum of 31 tunnels. When you define multiple preferences for a destination, you increase the probability of a successful connection.

   host1(config-tunnel-group-tunnel)#preference 5

6. (Optional) Specify an authentication password for the tunnel.

   host1(config-tunnel-group-tunnel)#password temporary

   NOTE: If you specify a password for the LAC, the router requires that the peer (the LNS) authenticate itself to the router. In this case, if the peer fails to authenticate itself, the tunnel terminates.

7. (Optional) Specify a hostname for the LAC end of the tunnel.

   The LAC sends the hostname to the LNS when communicating to the LNS about the tunnel. The hostname can be up to 64 characters (no spaces).

   host1(config-tunnel-group-tunnel)#client-name host4.

   NOTE: If the LNS does not accept tunnels from unknown hosts, and if no hostname is specified, the LAC uses the router name as the hostname.

8. (Optional) Specify a server name for the LNS.

This name specifies the hostname expected from the peer (the LNS) when you set up a tunnel. When this name is specified, the peer must identify itself with this name during tunnel startup. Otherwise, the tunnel is terminated. The server name can be up to 64 characters (no spaces).

```
host1(config-tunnel-group-tunnel)#server-name boston
```

9. (Optional) Specify a source IP address for the LAC tunnel endpoint. All L2TP packets sent to the peer use this source address.

   By default, the router uses the virtual router's router ID as the source address. You can override this behavior for an L2TP tunnel by specifying a source address. If you do specify a source address, use the address of a stable IP interface (for example, a loopback interface). Make sure that the address is configured in the virtual router for this domain map, and that the address is reachable by the peer.

   ```
   host1(config-tunnel-group-tunnel)#source-address 192.0.3.3
   ```

10. Specify a tunnel identification.

    ```
    host1(config-tunnel-group-tunnel)#identification acton
    ```

    The router groups L2TP sessions with the same tunnel identification into the same tunnel. This occurs only when both the destination (virtual router, IP address) and the ID are the same.

11. Specify a medium type for the tunnel. (L2TP supports only IP version 4 [IPv4].)

    ```
    host1(config-tunnel-group-tunnel)#medium ipv4
    ```

12. Specify the L2TP tunnel type (RADIUS attribute 64, Tunnel-Type). Currently, the only supported value is L2TP.

    ```
    host1(config-tunnel-group-tunnel)#type l2tp
    ```

13. Verify the L2TP tunnel configuration.

```
host1(config)# show aaa domain-map
Domain: westford.com; router-name: default; ipv6-router-name: default

Tunnel
Tunnel   Tunnel         Tunnel        Tunnel   Tunnel    Tunnel    Tunnel
Client
 Tag      Peer          Source         Type    Medium   Password     Id
Name
------   ------------   -----------   ------   ------   ---------  ------
------
3        192.168.2.13   192.168.3.3   l2tp     ipv4     temporary  acton
host4

         Tunnel                Tunnel                     Tunnel
Tunnel   Server     Tunnel       Max                        Virtual
 Tag      Name    Preference   Sessions     Tunnel RWS     Router
------   ------   ----------   --------   --------------   -------
3        boston   5            0          system chooses   vr2

host1#show aaa tunnel-parameters
Tunnel password is 3&92k%b#q4
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
```

```
tunnel assignmentId format is assignmentId
aaa tunnel calling number format is descriptive
```

Related Documentation

- Mapping User Domain Names to L2TP Tunnels from Domain Map Tunnel Mode on page 44
- *aaa tunnel-group*
- address on page 84
- client-name on page 87
- identification on page 88
- medium ipv4 on page 112
- password on page 113
- preference on page 115
- router-name on page 125
- server-name on page 126
- source-address on page 128
- tunnel on page 129
- type on page 131

CHAPTER 10

Mechanisms for Selecting Tunnels for PPP User Sessions

Configuring LAC Tunnel Selection Parameters

This section presents the capabilities of the LAC's tunnel selection process. L2TP allows you to specify:

- Up to 31 destinations for a domain.
- Up to eight levels of preference. Preference indicates the order in which the router attempts to connect to the destinations specified for a domain. Zero (0) is the highest level of preference.
- Up to 31 destinations for a single preference level.

For information about setting up destinations and preference levels for a domain, see "Mapping a User Domain Name to an L2TP Tunnel Overview" on page 17.

When the E Series LAC determines that a PPP session should be tunneled, it selects a tunnel from a set of tunnels associated with either the PPP user or the PPP user's domain. The router provides the following methods for selecting tunnels:

- Tunnel selection failover between preference levels (the default behavior)
- Tunnel selection failover within a preference level
- Maximum sessions per tunnel
- Weighted load balancing

1. Configuring the Failover Between Preference Levels Method on page 52
2. Configuring the Failover Within a Preference Level Method on page 52
3. Configuring the Maximum Sessions per Tunnel on page 53
4. Configuring the Weighted Load Balancing Method on page 53

Configuring the Failover Between Preference Levels Method

When a user tries to log into a domain, in the default method, the router attempts to connect to a destination in that domain with the highest preference level. If more than one destination in the preference level is considered reachable, the router randomly selects a destination and attempts to contact it. If the router is unsuccessful, it marks the destination as unreachable and does not try to connect to that destination for five minutes. The router then moves to the next lower preference level and repeats the process. The router makes up to eight attempts to connect to a destination for a domain—one attempt for each preference level.

If all destinations at a preference level are marked as unreachable, the router chooses the destination that failed first and tries to make a connection. The key is to understand that the router chooses a single destination at each level of preference, even if all destinations have recently failed. Thus the 5-minute timer normally used to reinstate failed destinations is ignored under certain conditions.

For example, suppose you have three destinations for a domain: A, B, and C. You assign the following preferences:

- A, B, and C at preference 0
- A, B, and C at preference 1
- A, B, and C at preference 2

A, B, and C are all considered reachable.

If a PPP user tries to connect to the domain, suppose the router randomly selects destination A from preference 0. If this connection attempt fails, the router excludes destination A for 5 minutes and goes to the next level (preference 1). From here, it randomly selects destination B, one of the two remaining choices. If the second connection attempt also fails, the router excludes destination B, as well as destination A, and attempts to connect to destination C, the only destination available with preference 2. The router has had an opportunity to connect to every destination available for the domain.

Support for multiple destinations affects the procedure for mapping a user domain name to an L2TP tunnel. To learn how to complete this mapping, see "Mapping a User Domain Name to an L2TP Tunnel Overview" on page 17.

- To enable tunnel selection failover between preference levels:

  This tunnel selection method is the default method. If you do not set any tunnel selection parameters, the router uses this method.

Configuring the Failover Within a Preference Level Method

You use the **l2tp fail-over-within-preference** command to enable tunnel selection failover within a preference level. In this selection method, if the router tries to connect to a destination and is unsuccessful, it selects a new destination at the same preference level. If all destinations at a preference level are marked as unreachable, the router does not

attempt to connect to a destination at that level. It drops to the next lower preference level to select a destination.

If all destinations at all preference levels are marked as unreachable, the router chooses the destination that failed first and tries to make a connection. If the connection fails, the router rejects the PPP user session without attempting to contact the remote router.

For example, suppose there are four tunnels for a domain: A, B, C, and D. All tunnels are considered reachable, and the preference levels are assigned as follows:

- A and B at preference 0
- C and D at preference 1

When the router attempts to connect to the domain, suppose it randomly selects tunnel B from preference 0. If it fails to connect to tunnel B, the router excludes tunnel B for five minutes and attempts to connect to tunnel A. If this attempt also fails, the router drops to preference 1. Then suppose the router selects tunnel C. If it also fails to connect to tunnel C, the router excludes tunnel C for five minutes and attempts to connect to tunnel D.

- To enable tunnel selection failover within a preference level:

```
host1(config)#l2tp fail-over-within-preference
```

Configuring the Maximum Sessions per Tunnel

You can configure the maximum number of sessions per tunnel, either through a RADIUS server or the command-line interface. If you set the maximum sessions per tunnel parameter, the router takes the setting into consideration when it selects a tunnel. If a randomly selected tunnel has a current session count equal to its maximum session count, the router does not attempt to contact that tunnel. Instead, it makes an alternate tunnel selection from the set of reachable tunnels at the same preference level. If no additional reachable tunnels exist at the current preference level, the router drops to the next lower preference level to make the next selection. This process is consistent, regardless of which fail-over scheme is currently running on the router. A tunnel without a configured maximum sessions value has no upper limit on the number of sessions it can support.

The router uses a default value of 0 (zero), which allows unlimited sessions in the tunnel.

- To configure the maximum sessions per tunnel.

```
host1(config)#aaa domain-map lacOne
host1(config-domain-map)#tunnel 1
host1(config-domain-map-tunnel)#max-sessions 1500
```

Configuring the Weighted Load Balancing Method

With the weighted load-balancing method, the router uses the maximum sessions per tunnel to choose among multiple tunnels that share the same preference level.

The weight of a tunnel is proportional to its maximum session limit and the maximum session limits of the other tunnels at the same preference level. The tunnel with the largest maximum session value has the largest weight; the tunnel with the next largest maximum session value has the next largest weight, down to the tunnel with the smallest maximum session value that has the smallest weight. The router uses a round-robin tunnel selection method by default.

- To configure the router to base tunnel selection within a preference level on the maximum sessions per tunnel.

  host1(config)#**l2tp weighted-load-balancing**

CHAPTER 11

L2TP Destination Lockout Feature

Managing Address Changes Received from Remote Endpoints

A remote endpoint can use the Start-Control-Connection-Reply (SCCRP) packets that it sends to the E Series LAC to change the address that the LAC uses to communicate with the endpoint. By default, the LAC accepts the change and uses the new address to communicate with the endpoint. However, you can configure the LAC to ignore or reject the requested change. Setting up the LAC to ignore address changes in SCCRP packets enables the router to construct tunnels with separate receive and transmit addresses and to avoid problems due to a misconfiguration. Three possible configurations are available:

- Default configuration—The E Series LAC accepts the change from the endpoint. The LAC then sends all subsequent packets to, and accepts packets from, the new address.
- Ignore configuration (specified by the **l2tp ignore-transmit-address-change** command)—The LAC continues to send packets to the original address but accepts packets from the new address.

  ```
  host1(config)#l2tp ignore-transmit-address-change
  Use the ip-address or udp-port keyword to ignore the specific address component. Omit
    the keywords to ignore the entire address change in the SCCRP packet.
  ```

- Reject configuration (specified by the **l2tp reject-transmit-address-change** command)—The LAC sends a Stop-Control-Connection-Notification (StopCCN) to the original address, then terminates the connection to the endpoint.

  ```
  host1(config)#l2tp reject-transmit-address-change ip-address
  ```

  Use the **ip-address** or **udp-port** keyword to reject the specific address component. Omit the keywords to reject the entire address change in the SCCRP packet.

NOTE: When an L2TP hello message contains a non-zero value in the Reserved Bits field of the L2TP message header, and the LAC rejects the change in the endpoint address by sending a StopCCN to the original address, the Result Code field contains the value of 2 and the Error Code field contains the value of 3. The Result code value denotes a generic error, while the Error code value denotes that one of the field values was out of range or the Reserved Bits field was non-zero in the StopCCN message sent from the LAC to the endpoint.

The reject specification takes precedence over the ignore specification.

The router accepts a change in receive address only once, during the tunnel establishment phase, and only on an SCCRP packet. Subsequent changes result in the router dropping packets. Any changes do not affect established tunnels.

Use the **show l2tp** command to display the SCCRP address change configuration.

Related Documentation

- *l2tp ignore-transmit-address-change*
- *l2tp reject-transmit-address-change*

Configuring LAC Tunnel Selection Parameters

This section presents the capabilities of the LAC's tunnel selection process. L2TP allows you to specify:

- Up to 31 destinations for a domain.
- Up to eight levels of preference. Preference indicates the order in which the router attempts to connect to the destinations specified for a domain. Zero (0) is the highest level of preference.
- Up to 31 destinations for a single preference level.

For information about setting up destinations and preference levels for a domain, see "Mapping a User Domain Name to an L2TP Tunnel Overview" on page 17.

When the E Series LAC determines that a PPP session should be tunneled, it selects a tunnel from a set of tunnels associated with either the PPP user or the PPP user's domain. The router provides the following methods for selecting tunnels:

- Tunnel selection failover between preference levels (the default behavior)
- Tunnel selection failover within a preference level
- Maximum sessions per tunnel
- Weighted load balancing

1. Configuring the Failover Between Preference Levels Method on page 57
2. Configuring the Failover Within a Preference Level Method on page 57

3. Configuring the Maximum Sessions per Tunnel on page 58
4. Configuring the Weighted Load Balancing Method on page 58

Configuring the Failover Between Preference Levels Method

When a user tries to log into a domain, in the default method, the router attempts to connect to a destination in that domain with the highest preference level. If more than one destination in the preference level is considered reachable, the router randomly selects a destination and attempts to contact it. If the router is unsuccessful, it marks the destination as unreachable and does not try to connect to that destination for five minutes. The router then moves to the next lower preference level and repeats the process. The router makes up to eight attempts to connect to a destination for a domain—one attempt for each preference level.

If all destinations at a preference level are marked as unreachable, the router chooses the destination that failed first and tries to make a connection. The key is to understand that the router chooses a single destination at each level of preference, even if all destinations have recently failed. Thus the 5-minute timer normally used to reinstate failed destinations is ignored under certain conditions.

For example, suppose you have three destinations for a domain: A, B, and C. You assign the following preferences:

- A, B, and C at preference 0
- A, B, and C at preference 1
- A, B, and C at preference 2

A, B, and C are all considered reachable.

If a PPP user tries to connect to the domain, suppose the router randomly selects destination A from preference 0. If this connection attempt fails, the router excludes destination A for 5 minutes and goes to the next level (preference 1). From here, it randomly selects destination B, one of the two remaining choices. If the second connection attempt also fails, the router excludes destination B, as well as destination A, and attempts to connect to destination C, the only destination available with preference 2. The router has had an opportunity to connect to every destination available for the domain.

Support for multiple destinations affects the procedure for mapping a user domain name to an L2TP tunnel. To learn how to complete this mapping, see "Mapping a User Domain Name to an L2TP Tunnel Overview" on page 17.

- To enable tunnel selection failover between preference levels:

  This tunnel selection method is the default method. If you do not set any tunnel selection parameters, the router uses this method.

Configuring the Failover Within a Preference Level Method

You use the **l2tp fail-over-within-preference** command to enable tunnel selection failover within a preference level. In this selection method, if the router tries to connect to a

destination and is unsuccessful, it selects a new destination at the same preference level. If all destinations at a preference level are marked as unreachable, the router does not attempt to connect to a destination at that level. It drops to the next lower preference level to select a destination.

If all destinations at all preference levels are marked as unreachable, the router chooses the destination that failed first and tries to make a connection. If the connection fails, the router rejects the PPP user session without attempting to contact the remote router.

For example, suppose there are four tunnels for a domain: A, B, C, and D. All tunnels are considered reachable, and the preference levels are assigned as follows:

- A and B at preference 0
- C and D at preference 1

When the router attempts to connect to the domain, suppose it randomly selects tunnel B from preference 0. If it fails to connect to tunnel B, the router excludes tunnel B for five minutes and attempts to connect to tunnel A. If this attempt also fails, the router drops to preference 1. Then suppose the router selects tunnel C. If it also fails to connect to tunnel C, the router excludes tunnel C for five minutes and attempts to connect to tunnel D.

- To enable tunnel selection failover within a preference level:

  host1(config)#l2tp fail-over-within-preference

Configuring the Maximum Sessions per Tunnel

You can configure the maximum number of sessions per tunnel, either through a RADIUS server or the command-line interface. If you set the maximum sessions per tunnel parameter, the router takes the setting into consideration when it selects a tunnel. If a randomly selected tunnel has a current session count equal to its maximum session count, the router does not attempt to contact that tunnel. Instead, it makes an alternate tunnel selection from the set of reachable tunnels at the same preference level. If no additional reachable tunnels exist at the current preference level, the router drops to the next lower preference level to make the next selection. This process is consistent, regardless of which fail-over scheme is currently running on the router. A tunnel without a configured maximum sessions value has no upper limit on the number of sessions it can support.

The router uses a default value of 0 (zero), which allows unlimited sessions in the tunnel.

- To configure the maximum sessions per tunnel.

  host1(config)#aaa domain-map lacOne
  host1(config-domain-map)#tunnel 1
  host1(config-domain-map-tunnel)#max-sessions 1500

Configuring the Weighted Load Balancing Method

With the weighted load-balancing method, the router uses the maximum sessions per tunnel to choose among multiple tunnels that share the same preference level.

The weight of a tunnel is proportional to its maximum session limit and the maximum session limits of the other tunnels at the same preference level. The tunnel with the largest maximum session value has the largest weight; the tunnel with the next largest maximum session value has the next largest weight, down to the tunnel with the smallest maximum session value that has the smallest weight. The router uses a round-robin tunnel selection method by default.

- To configure the router to base tunnel selection within a preference level on the maximum sessions per tunnel.

  host1(config)#**l2tp weighted-load-balancing**

CHAPTER 12

Generating RX Speed Attribute Value Pair (AVP) on the LAC

Configuring the RX Speed on the LAC

You can configure the E Series LAC to generate the L2TP RX Connect-Speed AVP [38], which is transmitted to the LNS in the Incoming-Call-Connected message. The AVP carries one of the following subscriber access interface speeds based on the configuration:

- L2C RAM actual upstream rate
- Configured advisory receive speed
- Calculated transmit speed

By default, the receive speed is set equal to the calculated transmit speed and the generation of the RX Connect-Speed AVP is suppressed. The AVP can be used to generate the RADIUS Connect-Info attribute [77] on the LNS.

To set up the router to generate the RX Connect-Speed AVP [38], perform all or any one of the following steps:

- Configure the advisory receive speed:

  NOTE: The configured advisory receive speed is sent in the RX Connect-Speed AVP, only if the generation of the AVP for transmitting the actual upstream rate is disabled.

  - On the ATM subinterface:

    host1(config-subif)#atm atm1483 advisory-rx-speed 2000

    For more information about configuring the advisory speed, see *Configuring ATM* in the *JunosE Link Layer Configuration Guide*.

  - On the VLAN subinterface:

    host1(config-subif)#vlan advisory-rx-speed 2000

- Enable generation of the RX Connect-Speed AVP when the receive speed is set equal to the calculated transmit speed.

NOTE: The calculated transmit speed is sent in the RX Connect-Speed AVP only if the advisory receive speed is not configured and the generation of the AVP for transmitting the actual upstream rate is disabled.

```
host1(config)#l2tp rx-connect-speed-when-equal
```

- Enable generation of the RX Connect-Speed AVP when you want to send the L2C RAM actual upstream rate in the AVP.

NOTE: The actual upstream rate is sent in the AVP even if the advisory receive speed is configured and the generation of the AVP is enabled for sending the calculated transmit speed.

```
host1(config)#l2tp rx-connect-speed-upstream-rate
```

Related Documentation

- *Transmission of the Subscriber Access Interface Speed to LNS Using the RX Connect-Speed AVP*
- *atm atm1483 advisory-rx-speed*
- *l2tp rx-connect-speed-upstream-rate*
- *l2tp rx-connect-speed-when-equal*
- *vlan advisory-rx-speed*

CHAPTER 13

Calling Number AVP in ICRQ Packets

Configuring Calling Number AVP Formats

The E Series LAC generates L2TP Calling Number AVP 22 for incoming-call request (ICRQ) packets that the LAC sends to the LNS. By default, the E Series LAC generates the Calling Number AVP 22 in descriptive format.

You can also prevent the E Series LAC from sending the Calling Number AVP in ICRQ packets.

NOTE: **You cannot change the L2TP Calling Number AVP on tunnel switched interfaces.**

You use the **aaa tunnel calling-number-format** command to configure the router to generate AVP 22 in any of the following formats. Agent-circuit-id is suboption 1 of the tags supplied by the PPPoE intermediate agent from the DSLAM. Agent-remote-id is suboption 2.

- descriptive—This is the default format, and includes the following elements:

  <interface ID> <delimit> <UID> <delimit> <interface description> <delimit> <connect info> <delimit> <PPPoE description>

- descriptive include-agent-circuit-id—This format includes the following elements:

  <interface ID> <delimit> <UID> <delimit> <interface description> <delimit> <connect info> <delimit> <PPPoE description> <delimit> <agent-circuit-id>

- descriptive include-agent-circuit-id include-agent-remote-id—This format includes the following elements:

  <interface ID> <delimit> <UID> <delimit> <interface description> <delimit> <connect info> <delimit> <PPPoE description> <delimit> <agent-circuit-id> <delimit> <agent-remote-id>

- descriptive include-agent-remote-id—This format includes the following elements:

<interface ID> <delimit> <UID> <delimit> <interface description> <delimit> <connect info> <delimit> <PPPoE description> <delimit> <agent-remote-id>

- fixed—This format is similar to the fixed format of RADIUS attribute 31 (Calling-Station-Id). If you set up the router to generate the Calling Number AVP in fixed format, the router formats the AVP to use a fixed format of up to 15 characters consisting of all ASCII fields, as follows (the maximum number of characters for each field is shown in brackets):
  - For ATM interfaces:
    <system name [4]> <slot [2]> <port [1]> <VPI [3]> <VCI [5]>
  - For Ethernet interfaces:
    <system name [4]> <slot [2]> <port [1]> <VLAN [8]>
  - Format for serial interfaces:
    <system name [4]> <slot [2]> <port [1]> <0 [8]>
  - Example—The following command configures the L2TP Calling Number AVP in fixed format:

    host1(config)#aaa tunnel calling-number-format fixed

    For example, when you configure this L2TP Calling Number AVP format on an E320 Broadband Services Router for an ATM interface on system name eastern, slot 14, adapter 1, port 2, VCI 3, and VPI 4, the virtual router displays the format in ASCII as '14' '2' '003' '00004'. The adapter number does not appear in this format.

- fixed-adapter-embedded—If you set up the router to generate the L2TP Calling Number AVP in fixed–adapter-embedded format, the router formats the AVP to use a fixed format of up to 15 characters consisting of all ASCII fields with a 1-byte *slot* field, 1-byte *adapter* field, and 1-byte *port* field:
  - Format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte)
    port (1 byte) *VPI* (3 bytes) *VCI* (5 bytes)
  - Format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte)
    port (1 byte) *VLAN* (8 bytes)
  - Format for serial interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte)
    port (1 byte) 0 (8 bytes)
  - For E120 and E320 Broadband Services Routers, *adapter* is the number of the bay in which the I/O adapter (IOA) resides, either 0 (representing the right IOA bay on the E120 router and the upper IOA bay on the E320 router) or 1 (representing the left IOA bay on the E120 router or the lower IOA bay on the E320 router). For ERX7xx models, ERX14xx models, and ERX310 Broadband Services Routers, which do not use IOAs, *adapter* is always shown as 0.

- Slot numbers 0 through 16 are shown as ASCII characters in the 1-byte slot field according to the following translation:

Slot Number	ASCII Character	Slot Number	ASCII Character
0	0	9	9
1	1	10	A
2	2	11	B
3	3	12	C
4	4	13	D
5	5	14	E
6	6	15	F
7	7	16	G
8	8	–	–

  For example, slot 16 is shown as the ASCII character uppercase G.

- Example—The following command configures the L2TP Calling Number AVP in fixed-adapter-embedded format:

  host1(config)#aaa tunnel calling-number-format fixed-adapter-embedded

  For example, when you configure this L2TP Calling Number AVP format on an E320 router for an ATM interface on system name eastern, slot 14, adapter 1, port 2, VCI 3, and VPI 4, the virtual router displays the format in ASCII as ‘E’ ‘1’ ‘2’ ‘003’ ‘00004’.

- fixed-adapter-new-field—If you set up the router to generate the L2TP Calling Number AVP in fixed–adapter-embedded-new-field format, the router formats the AVP to use a fixed format of up to 17 characters consisting of all ASCII fields with a 2-byte *slot* field, 1-byte *adapter* field, and 2-byte *port* field:

  - Format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte)
    port (2 bytes) *VPI* (3 bytes) *VCI* (5 bytes)
  - Format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte)
    port (2 bytes) *VLAN* (8 bytes)
  - Format for serial interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte)
    port (2 bytes) 0 (8 bytes)
  - Slot numbers 0 through 16 are shown as integers in the 2-byte *slot* field.

- Example—The following command configures the L2TP Calling Number AVP in fixed-adapter-new-field format:

  host1(config)#aaa tunnel calling-number-format fixed-adapter-new-field

  For example, when you configure this L2TP Calling Number AVP format on an E320 router for an ATM interface on system name eastern, slot 14, adapter 1, port 2, VCI 3, and VPI 4, the virtual router displays the format in ASCII as '14' '1' '02' '003' '00004'.

- include-agent-circuit-id format—This format includes the following element:

  <agent-circuit-id>

- include-agent-circuit-id include-agent-remote-id format—This format includes the following elements:

  <agent-circuit-id> <delimit> <agent-remote-id>

- include-agent-remote-id format—This format includes the following element:

  <agent-remote-id>

- stacked—This format includes a 4-byte stacked VLAN (S-VLAN) ID in the fixed, fixed-adapter-embedded, and fixed-adapter-new-field Calling Number AVP formats for Ethernet interfaces. The S-VLAN ID is displayed in decimal format in the range 0–4095. By default, these formats do not include the S-VLAN ID unless you specify the optional **stacked** keyword.

  NOTE: The use of the **stacked** keyword is not supported for VLAN subinterfaces based on agent-circuit-identifier information, otherwise known as ACI VLANs. When you issue the **aaa tunnel calling-number-format fixed stacked**, **aaa tunnel calling-number-format fixed-adapter-embedded stacked**, or **aaa tunnel calling-number-format fixed-adapter-new-field stacked** command for an ACI VLAN, the values that appear in the 4-byte S-VLAN ID and 4-byte VLAN ID fields are incorrect.

  - Format for Ethernet interfaces that use **fixed**:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
  - Format for Ethernet interfaces that use **fixed-adapter-embedded**:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
  - Format for Ethernet interfaces that use **fixed-adapter-new-field**:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
  - The S-VLAN ID field in the Calling Number AVP is set to 0 (zero) if you do not specify the optional **stacked** keyword, or if you specify the optional **stacked** keyword but the Ethernet interface does not have an S-VLAN ID.
  - Example—The following command configures the L2TP Calling Number AVP in fixed-adapter-new-field format for an Ethernet interface with an S-VLAN ID:

```
host1(config)#aaa tunnel calling-number-format fixed-adapter-new-field stacked
```

For example, when you configure this Calling-Station-Id format on an E320 router for an Ethernet interface on system name western, slot 4, adapter 1, port 3, S-VLAN ID 8, and VLAN ID 12, the virtual router displays the format in ASCII as 'west' '04' '1' '03' '0008' '0012'.

Tasks for configuring the L2TP Calling Number AVP 22 include:

- Calling Number AVP 22 Configuration Tasks on page 67
- Configuring the Fallback Format on page 67
- Disabling the Calling Number AVP on page 71

Calling Number AVP 22 Configuration Tasks

To set up the router to generate Calling Number AVP 22 for an Ethernet interface in fixed format that includes both an S-VLAN ID and a VLAN ID:

1. Set the calling number format of the tunnel to **fixed**, and specify the optional **stacked** keyword to include the S-VLAN ID.

   ```
   host1(config)#aaa tunnel calling-number-format fixed stacked
   ```

2. Set the format of the RADIUS Calling-Station-Id to **fixed-format**, and specify the optional **stacked** keyword to include the S-VLAN ID.

   ```
   host1(config)#radius calling-station-format fixed-format stacked
   ```

If you use a RADIUS server to authenticate the L2TP tunnel parameters, you must configure the format for both the L2TP Calling Number AVP 22 (by using the **aaa tunnel calling-number-format** command) and the RADIUS Calling-Station-ID [31] attribute (by using the **radius calling-station-format** command).

However, if you use an AAA domain map to authenticate the L2TP tunnel parameters, you need configure only the L2TP Calling Number AVP 22 format by using the **aaa tunnel calling-number-format** command. You need not configure the format of the RADIUS Calling-Station-ID [31] attribute in this case.

Configuring the Fallback Format

You can configure a fallback AVP 22 format. The E Series LAC uses the fallback format to generate the L2TP Calling Number AVP 22 in the event that the PPPoE agent ID is null or unavailable. The LAC uses the fallback format only when the configured calling number format includes either or both of the agent-circuit-id and agent-remote-id suboptions.

The calling number format determines what element triggers use of the fallback format, as shown in the following table:

Calling Number Format	Fallback Trigger
agent-circuit-id	agent-circuit-id is empty

Calling Number Format	Fallback Trigger
agent-circuit-id include-agent-remote-id	Both agent-circuit-id and agent-remote-id are empty.
agent-remote-id	agent-remote-id is empty
descriptive include-agent-circuit-id	agent-circuit-id is empty
descriptive include-agent-circuit-id include-agent-remote-id	Both agent-circuit-id and agent-remote-id are empty.
descriptive include-agent-remote-id	agent-remote-id is empty

You use the **aaa tunnel calling-number-format-fallback** command to configure the router to generate any of the following fallback AVP 22 formats:

- descriptive—This is the default fallback AVP 22 format, and includes the following elements:

  <interface ID> <delimit> <UID> <delimit> <interface description> <delimit> <connect info> <delimit> <PPPoE description>

- fixed—This format is similar to the fixed format of RADIUS attribute 31 (Calling-Station-Id). If you set up the router to generate the fallback AVP 22 in fixed format, the router formats the AVP to use a fixed format of up to 15 characters consisting of all ASCII fields, as follows (the maximum number of characters for each field is shown in brackets):

  - Fallback format for ATM interfaces:
    <system name [4]> <slot [2]> <port [1]> <VPI [3]> <VCI [5]>
  - Fallback format for Ethernet interfaces:
    <system name [4]> <slot [2]> <port [1]> <VLAN [8]>
  - Fallback format for serial interfaces:
    <system name [4]> <slot [2]> <port [1]> <0 [8]>
  - Example—The following command configures the fallback AVP 22 in fixed format:

    host1(config)#aaa tunnel calling-number-format-fallback fixed

    For example, when you configure this fallback format on an E320 router for an ATM interface on system name eastern, slot 14, adapter 1, port 2, VCI 3, and VPI 4, the virtual router displays the format in ASCII as '14' '2' '003' '00004'. The adapter number does not appear in this format.

- fixed-adapter-embedded—If you set up the router to generate the fallback AVP 22 in fixed–adapter-embedded format, the router formats the AVP to use a fixed format of up to 15 characters consisting of all ASCII fields with a 1-byte *slot* field, 1-byte *adapter* field, and 1-byte *port* field:

- Fallback format for ATM interfaces:
  systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte)
  port (1 byte) *VPI* (3 bytes) *VCI* (5 bytes)
- Fallback format for Ethernet interfaces:
  systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte)
  port (1 byte) *VLAN* (8 bytes)
- Fallback format for serial interfaces:
  systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte)
  port (1 byte) 0 (8 bytes)
- For E120 routers and E320 routers, *adapter* is the number of the bay in which the I/O adapter (IOA) resides, either 0 (representing the right IOA bay on the E120 router and the upper IOA bay on the E320 router) or 1 (representing the left IOA bay on the E120 router or the lower IOA bay on the E320 router). For ERX7xx models, ERX14xx models, and ERX310 routers, which do not use IOAs, *adapter* is always shown as 0.
- Slot numbers 0 through 16 are shown as ASCII characters in the 1-byte slot field according to the following translation:

Slot Number	ASCII Character	Slot Number	ASCII Character
0	0	9	9
1	1	10	A
2	2	11	B
3	3	12	C
4	4	13	D
5	5	14	E
6	6	15	F
7	7	16	G
8	8	–	–

  For example, slot 16 is shown as the ASCII character uppercase G.
- Example—The following command configures the fallback AVP 22 in fixed-adapter-embedded format:

  host1(config)#aaa tunnel calling-number-format-fallback fixed-adapter-embedded

  For example, when you configure this fallback format on an E320 router for an ATM interface on system name eastern, slot 14, adapter 1, port 2, VCI 3, and VPI 4, the virtual router displays the format in ASCII as ‘E’ ‘1’ ‘2’ ‘003’ ‘00004’.

- fixed-adapter-new-field—If you set up the router to generate the fallback AVP 22 in fixed–adapter-embedded-new-field format, the router formats the AVP to use a fixed format of up to 17 characters consisting of all ASCII fields with a 2-byte *slot* field, 1-byte *adapter* field, and 2-byte *port* field:
  - Fallback format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte)
    port (2 bytes) *VPI* (3 bytes) *VCI* (5 bytes)
  - Fallback format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte)
    port (2 bytes) *VLAN* (8 bytes)
  - Fallback format for serial interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte)
    port (2 bytes) 0 (8 bytes)
  - Slot numbers 0 through 16 are shown as integers in the 2-byte *slot* field.
  - Example—The following command configures the fallback AVP 22 in fixed-adapter-new-field format:

    host1(config)#aaa tunnel calling-number-format-fallback fixed-adapter-new-field

    For example, when you configure this fallback format on an E320 router for an ATM interface on system name eastern, slot 14, adapter 1, port 2, VCI 3, and VPI 4, the virtual router displays the format in ASCII as '14' '1' '02' '003' '00004'.

- stacked—This format includes a 4-byte stacked VLAN (S-VLAN) ID in the fixed, fixed-adapter-embedded, and fixed-adapter-new-field fallback AVP 22 formats for Ethernet interfaces. The S-VLAN ID is displayed in decimal format in the range 0–4095. By default, these formats do not include the S-VLAN ID unless you specify the optional **stacked** keyword.

  NOTE: The use of the **stacked** keyword is not supported for VLAN subinterfaces based on agent-circuit-identifier information, otherwise known as ACI VLANs. When you issue the **aaa tunnel calling-number-format-fallback fixed stacked**, **aaa tunnel calling-number-format-fallback fixed-adapter-embedded stacked**, or **aaa tunnel calling-number-format-fallback fixed-adapter-new-field stacked** command for an ACI VLAN, the values that appear in the 4-byte S-VLAN ID and 4-byte VLAN ID fields are incorrect.

  - Fallback format for Ethernet interfaces that use **fixed**:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
  - Fallback format for Ethernet interfaces that use **fixed-adapter-embedded**:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
  - Fallback format for Ethernet interfaces that use **fixed-adapter-new-field**:

systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *S-VLAN* (4 bytes) *VLAN* (4 bytes)

- The S-VLAN ID field in the fallback AVP 22 is set to 0 (zero) if you do not specify the optional **stacked** keyword, or if you specify the optional **stacked** keyword but the Ethernet interface does not have an S-VLAN ID.
- Example—The following command configures the fallback AVP 22 in fixed-adapter-new-field format for an Ethernet interface with an S-VLAN ID:

  host1(config)#aaa tunnel calling-number-format-fallback fixed-adapter-new-field stacked

  For example, when you configure this fallback format on an E320 router for an Ethernet interface on system name western, slot 4, adapter 1, port 3, S-VLAN ID 8, and VLAN ID 12, the virtual router displays the format in ASCII as ‘west’ ‘04’ ‘1’ ‘03’ ‘0008’ ‘0012’.

Disabling the Calling Number AVP

You can use the **l2tp disable calling-number-avp** command to prevent the E Series LAC from sending the Calling Number AVP in ICRQ packets. You use this command in special situations where you do not want the LAC to send this AVP.

- To prevent the LAC from sending the Calling Number AVP:

  host1(config)#l2tp disable calling-number-avp

For more information about setting up the router to generate Calling Number AVP 22 in a format that includes either or both of the agent-circuit-id and agent-remote-id suboptions of the tags supplied by the PPPoE intermediate agent, see *Configuring PPPoE Remote Circuit ID Capture* in the *JunosE Link Layer Configuration Guide* .

Calling Number AVP 22 Configuration Examples

The following examples show how you can synchronize the contents of RADIUS Calling-Station-Id (Attribute 31) and L2TP Calling-Number (AVP 22).

- To send the PPPoE agent-circuit-id in RADIUS Attribute 31 and L2TP AVP 22 and specify that the fixed format is used when the PPPoE agent-circuit-id is unavailable, issue the following commands:

```
host1(config)#radius calling-station-format fixed-format
host1(config)#radius remote-circuit-id-delimiter #
host1(config)#radius override calling-station-id remote-circuit-id
host1(config)#radius remote-circuit-id-format agent-circuit-id
host1(config)#aaa tunnel calling-number-format include-agent-circuit-id
host1(config)#aaa tunnel calling-number-format-fallback fixed
```

- To send the PPPoE agent-circuit-id and agent-remote-id in RADIUS Attribute 31 and L2TP AVP 22 and specify that the fixed format is used when both PPPoE agent-circuit-id and agent-remote-id are unavailable, issue the following commands:

```
host1(config)#radius calling-station-format fixed-format
host1(config)#radius remote-circuit-id-delimiter #
host1(config)#radius override calling-station-id remote-circuit-id
host1(config)#radius remote-circuit-id-format agent-circuit-id agent-remote-id
host1(config)#aaa tunnel calling-number-format include-agent-circuit-id
  include-agent-remote-id
host1(config)#aaa tunnel calling-number-format-fallback fixed
```

CHAPTER 14

Configuration Commands

aaa domain-map

Syntax aaa domain-map *domainName*
[*routerName* [loopback *interfaceNumber* | *ipAddress ipMask*]]

no aaa domain-map *domainName*

Release Information Command introduced before JunosE Release 7.1.0.
ipAddress and *ipMask* variables added in JunosE Release 9.0.0.

Description Maps a user domain name to a virtual router. When you specify only the domain name, the command sets the mode to Domain Map Configuration. The **no** version deletes the map entry.

Options
- *domainName*—User domain name; specify the domain name *none* to assign users without domains to a specific virtual router.
- *routerName*—Router name associated with the domain name
- loopback—Specifies the loopback interface
- *interfaceNumber*—Interface number in the range 0–32000
- *ipAddress*—IP address of the local interface
- *ipMask*—IPv4 address mask of the local interface

Mode Global Configuration

aaa tunnel calling-number-format-fallback

Syntax aaa tunnel calling-number-format-fallback
{ descriptive |
fixed [stacked] |
fixed-adapter-embedded [stacked] |
fixed-adapter-new-field [stacked] }

no aaa tunnel calling-number-format-fallback

Release Information Command introduced in JunosE Release 8.1.0.
fixed-adapter-embedded, **fixed-adapter-new-field**, and **stacked** keywords added in JunosE Release 10.0.0.

Description Configures the fallback format for the tunnel calling number to be passed by the E Series L2TP access concentrator (LAC) to the L2TP network server (LNS) in the L2TP Calling Number attribute value pair (AVP) 22 when the PPPoE agent circuit ID is null or unavailable. The fallback format is used only when the configured calling number format includes either or both of the agent-circuit-id and agent-remote-id suboptions. The **no** version restores the default fallback format, descriptive.

Options

- descriptive—Configures the fallback format in descriptive format that includes only interface information
- fixed—Configures the fallback format in a fixed format of up to 15 characters consisting of all ASCII fields, similar to the fixed format of RADIUS attribute 31 (Calling-Station-Id):
  - Fallback format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VPI* (3 bytes)
    VCI (5 bytes)
  - Fallback format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VLAN* (8 bytes)
  - Fallback format for serial interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) 0 (8 bytes)
  - In the case of PPP terminated from LNS, the Calling-Station-Id attribute is the value passed as the calling-station AVP.
- fixed-adapter-embedded—Configures the fallback format in a fixed format of up to 15 characters consisting of all ASCII fields with a 1-byte *slot* field, 1-byte *adapter* field, and 1-byte *port* field:
  - Fallback format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte)
    VPI (3 bytes) *VCI* (5 bytes)
  - Fallback format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte)
    VLAN (8 bytes)
  - Fallback format for serial interfaces:

systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) 0 (8 bytes)

- For E120 routers and E320 routers, *adapter* is the number of the bay in which the I/O adapter (IOA) resides, either 0 (representing the right IOA bay on the E120 router and the upper IOA bay on the E320 router) or 1 (representing the left IOA bay on the E120 router or the lower IOA bay on the E320 router). For ERX7xx models, ERX14xx models, and ERX310 routers, which do not use IOAs, *adapter* is always shown as 0.
- Slot numbers 0 through 16 are shown as ASCII characters in the 1-byte slot field.

- fixed-adapter-new-field—Configures the fallback format in a fixed format of up to 17 characters consisting of all ASCII fields with a 2-byte *slot* field, 1-byte *adapter* field, and 2-byte *port* field:
  - Fallback format for ATM interfaces: *systemName* (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *VPI* (3 bytes) *VCI* (5 bytes)
  - Fallback format for Ethernet interfaces: *systemName* (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *VLAN* (8 bytes)
  - Fallback format for serial interfaces: *systemName* (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) 0 (8 bytes)
  - For E120 routers and E320 routers, *adapter* is the number of the bay in which the IOA resides, either 0 or 1. For ERX7xx models, ERX14xx models, and ERX310 routers, which do not use IOAs, *adapter* is always shown as 0.
  - Slot numbers 0 through 16 are shown as integers in the 2-byte *slot* field.
- stacked—Includes a 4-byte stacked VLAN (S-VLAN) ID in the fixed, fixed-adapter-embedded, and fixed-adapter-new-field fallback formats for Ethernet interfaces; by default, these formats do not include the S-VLAN ID unless you specify the optional **stacked** keyword:
  - Fallback format for Ethernet interfaces that use **fixed**: *systemName* (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
  - Fallback format for Ethernet interfaces that use **fixed-adapter-embedded**: *systemName* (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
  - Fallback format for Ethernet interfaces that use **fixed-adapter-new-field**: *systemName* (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *S-VLAN* (4 bytes) *VLAN* (4 bytes)

Mode Global Configuration

aaa tunnel assignment-id-format

Syntax aaa tunnel assignment-id-format { assignmentId | client-server-id }

no aaa tunnel assignment-id-format

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets the format for the tunnel assignment ID. The **no** version sets the tunnel assignment ID to the default, assignmentId.

Options
- assignmentId—Configures the format to be assignmentId only
- client-server-id—Configures the format to be a combination of clientAuthId + serverAuthId + assignmentId

Mode Global Configuration

aaa tunnel client-name

Syntax aaa tunnel client-name *name*

no aaa tunnel client-name

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the default tunnel client name. If the tunnel client name is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default name. The **no** version deletes the client name.

Options
- *name*—Default tunnel client name; a string of up to 32 characters

Mode Global Configuration

aaa tunnel ignore

Syntax aaa tunnel ignore { nas-port | nas-port-type } { enable | disable }

no aaa tunnel ignore { nas-port | nas-port-type }

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies whether to use the tunnel peer's NAS-Port [5] and NAS-Port-Type [61] attributes. The **no** version negates the command or restores the default of enable.

Options

- nas-port—Configures the tunnel peer's supplied nas-port value
- nas-port-type—Configures the tunnel peer's supplied nas-port-type value
- enable—Implements the feature; this is the default setting
- disable—Disables the feature

Mode Global Configuration

aaa tunnel password

Syntax aaa tunnel password *name*

no aaa tunnel password

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the default tunnel password. If the tunnel password is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default password. The **no** version deletes the password.

Options
- *name*—Default tunnel password; a string of up to 32 characters

Mode Global Configuration

aaa tunnel calling-number-format

Syntax

aaa tunnel calling-number-format
{ descriptive [include-agent-circuit-id] [include-agent-remote-id] |
fixed [stacked] |
fixed-adapter-embedded [stacked] |
fixed-adapter-new-field [stacked] |
include-agent-circuit-id [include-agent-remote-id] |
include-agent-remote-id }

no aaa tunnel calling-number-format

Release Information

Command introduced before JunosE Release 7.1.0.
include-agent-circuit-id and **include-agent-remote-id** keywords added in JunosE Release 8.1.0.
stacked keyword added in JunosE Release 9.3.0.
fixed-adapter-embedded and **fixed-adapter-new-field** keywords added in JunosE Release 10.0.0.

Description

Configures the format used by the E Series L2TP access concentrator (LAC) to generate the L2TP Calling Number attribute value pair (AVP) 22 that it passes to the L2TP network server (LNS). Available formats include different fixed formats and several formats that include either or both of the agent-circuit-id (suboption 1) and agent-remote-id (suboption 2) suboptions of the PPPoE intermediate agent tags. The **no** version restores the default calling number format, descriptive.

Options

- descriptive—Formats calling number AVP in descriptive format that includes only interface information
- descriptive include-agent-circuit-id—Formats calling number AVP in descriptive format to include interface information and the agent-circuit-id suboption
- descriptive include-agent-circuit-id include-agent-remote-id—Formats calling number AVP in descriptive format to include interface information and both the agent-circuit-id and agent-remote-id suboptions
- descriptive include-agent-remote-id—Formats calling number AVP in descriptive format to include interface information and the agent-remote-id
- fixed—Formats calling number AVP to use a fixed format of up to 15 characters consisting of all ASCII fields, similar to the fixed format of RADIUS attribute 31 (Calling-Station-Id):
  - Format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VPI* (3 bytes) *VCI* (5 bytes)
  - Format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VLAN* (8 bytes)
  - Format for serial interfaces:

systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) 0 (8 bytes)

- In the case of PPP terminated from LNS, the Calling-Station-Id attribute is the value passed as the calling-station AVP.

- fixed-adapter-embedded—Formats calling number AVP to use a fixed format of up to 15 characters consisting of all ASCII fields with a 1-byte *slot* field, 1-byte *adapter* field, and 1-byte *port* field:
  - Format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *VPI* (3 bytes) *VCI* (5 bytes)
  - Format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *VLAN* (8 bytes)
  - Format for serial interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) 0 (8 bytes)
  - For E120 and E320 routers, *adapter* is the number of the bay in which the I/O adapter (IOA) resides, either 0 (representing the right IOA bay on the E120 router and the upper IOA bay on the E320 router) or 1 (representing the left IOA bay on the E120 router or the lower IOA bay on the E320 router). For ERX7xx models, ERX14xx models, and ERX310 routers, which do not use IOAs, *adapter* is always shown as 0.
  - Slot numbers 0 through 16 are shown as ASCII characters in the 1-byte slot field.
- fixed-adapter-new-field—Formats calling number AVP to use a fixed format of up to 17 characters consisting of all ASCII fields with a 2-byte *slot* field, 1-byte *adapter* field, and 2-byte *port* field:
  - Format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *VPI* (3 bytes) *VCI* (5 bytes)
  - Format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *VLAN* (8 bytes)
  - Format for serial interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) 0 (8 bytes)
  - For E120 routers and E320 routers, *adapter* is the number of the bay in which the IOA resides, either 0 or 1. For ERX7xx models, ERX14xx models, and ERX310 routers, which do not use IOAs, *adapter* is always shown as 0.
  - Slot numbers 0 through 16 are shown as integers in the 2-byte *slot* field.
- include-agent-circuit-id—Formats calling number AVP to include only the agent-circuit-id suboption
- include-agent-circuit-id include-agent-remote-id—Formats calling number AVP to include both the agent-circuit-id and agent-remote-id suboptions

- include-agent-remote-id—Formats calling number AVP to include only the agent-remote-id suboption
- stacked—Includes a 4-byte stacked VLAN (S-VLAN) ID in the fixed, fixed-adapter-embedded, and fixed-adapter-new-field calling number AVP formats for Ethernet interfaces; by default, these formats do not include the S-VLAN ID unless you specify the optional **stacked** keyword:
  - Format for Ethernet interfaces that use **fixed**: *systemName* (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
  - Format for Ethernet interfaces that use **fixed-adapter-embedded**: *systemName* (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
  - Format for Ethernet interfaces that use **fixed-adapter-new-field**: *systemName* (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *S-VLAN* (4 bytes) *VLAN* (4 bytes)

Mode Global Configuration

address

Syntax To set the tunnel endpoint address:

address *serverAddress*

no address

To configure RIP:

[no] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* }

To configure NAT address pool ranges:

[no] address *startIpAddress endIpAddress*

Release Information Command introduced before JunosE Release 7.1.0.

Description From Domain Map Tunnel Configuration mode, sets the tunnel endpoint address of an L2TP tunnel. The **no** version removes the address of the tunnel.

From Tunnel Group Tunnel Configuration mode, sets the tunnel endpoint address of an L2TP tunnel. The **no** version removes the address of the tunnel.

From Interface Configuration or Subinterface Configuration mode, configures RIP to run on the interface specified by the IP address or on an unnumbered interface. Uses the default values: send version is RIP version 1, receive version is RIP version 1 and version 2, authentication is not enabled. The **no** version deletes the RIP interface. Use the **address** commands to configure RIP attributes on the network.

From IP NAT Pool Configuration mode, configures NAT IP address pool ranges. The **no** version removes the range from the current NAT address pool.

Options

- *serverAddress*—IP address of the LNS endpoint
- *ipAddress*—Address of IP interface where RIP will be run
- unnumbered—Specifies that RIP will be run on an unnumbered interface
  - *interfaceType*—Interface type; see *Interface Types and Specifiers*
  - *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
- *startIpAddress*—Starting IP address (inclusive) of the NAT pool range you are creating
- *endIpAddress*—Ending IP address (inclusive) of the NAT pool range you are creating

Mode Address Family Configuration (RIP), Domain Map Tunnel Configuration, IP NAT Pool Configuration, Router Configuration (RIP), Tunnel Group Tunnel Configuration

bundled-group-id

Syntax [no] bundled-group-id *bundledGroupID*

Release Information Command introduced before JunosE Release 7.1.0.

Description Assigns a bundled group identifier when no endpoint discriminator is available for bundled sessions using an L2TP destination host profile. When multiple tunnel-service modules are installed in a router that is deployed as an LNS and the tunnel sessions carry MLPPP, the router can use the bundled group identifier when selecting a tunnel-service module for bundled sessions. The **no** version restores the default value, no assigned bundled group identifier.

NOTE: We recommend that you assign a bundled group identifier for bundled sessions only when you are certain that endpoint discriminators are unavailable to identify bundle membership.

Options

- *bundledGroupID*—Identifier for a bundled group in the range 0–4294967295

Mode L2TP Destination Profile Host Configuration

bundled-group-id-overrides-mlppp-ed

Syntax [no] bundled-group-id-overrides-mlppp-ed

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies that the router uses the bundled group identifier you assigned using the **bundled-group-id** command when selecting a tunnel-service module instead of any endpoint discriminator. The **no** version removes the override.

NOTE: We strongly recommend that you use this command only with the support of JTAC.

Mode L2TP Destination Profile Host Configuration

client-name

Syntax client-name *clientname*

no client-name

Release Information Command introduced before JunosE Release 7.1.0.

Description From Domain Map Tunnel Configuration or Tunnel Group Tunnel Configuration mode, sets a hostname for a tunnel that the LAC uses when communicating with the LNS about the tunnel. The **no** version removes the hostname from the tunnel.

NOTE: In Domain Map Tunnel Configuration mode, this command is replacing the *hostname* command. The *hostname* command may be removed completely from Domain Map Tunnel Configuration mode in a future release.

Options

- *clientname*—String of up to 64 characters (no spaces)

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

identification

Syntax identification *serverId*

no identification

Release Information Command introduced before JunosE Release 7.1.0.

Description From Domain Map Tunnel Configuration or Tunnel Group Tunnel mode, specifies the assignment ID of an L2TP tunnel. The **no** version removes the assignment ID from the tunnel.

Options
- *serverId*—L2TP tunnel assignment ID up to 32 characters

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel

default-upper-type mlppp

Syntax default-upper-type mlppp

no default-upper-type

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies that L2TP creates an MLPPP interface for the current LNS session when full LCP proxy data is not available. The **no** version deletes the MLPPP specification.

Mode L2TP Destination Profile Host Configuration

disable proxy lcp

Syntax [no] disable proxy lcp

Release Information Command introduced before JunosE Release 7.1.0.

Description Disables the proxy LCP parameter for the remote host. The **no** version enables the proxy LCP parameter for the remote host.

Mode L2TP Destination Profile Host Configuration

enable proxy authenticate

Syntax [no] enable proxy authenticate

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures proxy authenticate for a remote host. The **no** version removes proxy authenticate configuration from the remote host.

Mode L2TP Destination Profile Host Configuration

ip router-id

Syntax [no] ip router-id [*vrfName*] *ipAddress*

Release Information Command introduced before JunosE Release 7.1.0.

Description Establishes the IP address of a router. The **no** version removes the IP address assignment.

Options
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
- *ipAddress*—IP address of the router

Mode Global Configuration

Related Documentation
- *Configuring the Loopback Interface and Router ID for BGP for VPWS*
- *Configuring the Loopback Interface and Router ID for VPLS*

l2tp checksum

Syntax [no] l2tp checksum

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables the generation of a UDP data integrity checksum in data packets sent to an L2TP peer. The default setting is disabled. The **no** version disables the generation of the checksums.

Mode Global Configuration

l2tp destruct-timeout

Syntax l2tp destruct-timeout *seconds*

no l2tp destruct-timeout

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the maximum time for which the router maintains dynamic destinations, tunnels, and sessions that have terminated. When a subscriber is terminated, the server port that hosted the subscriber session is released after the dynamic interface destruct timeout is exceeded. The server port that is released is available for a new incoming-call request (ICRQ) packet that the LAC sends to the LNS. Until the time any server port is available to be used for a new incoming call, new ICRQ packets are denied because of a lack of system resources. The **no** version restores the default value, 600 seconds.

Options

- *seconds*—Time in the range 10–3600 seconds (1 hour)

Mode Global Configuration

l2tp destination profile

Syntax l2tp destination profile { *profileName* [[virtual-router *vrName*] ip address *ipAddress*] | [virtual-router *vrName*] ip address *ipAddress* }

no l2tp destination profile { *profileName* | [virtual-router *vrName*] ip address *ipAddress* }

Release Information Command introduced before JunosE Release 7.1.0.

Description Creates or accesses a destination profile that defines the location of a LAC. The **no** version removes the L2TP destination profile.

Options

- *profileName*—Name of the L2TP destination profile
- *vrName*—Name of the virtual router to be used to reach the destination (that is, the LAC). If you do not specify a virtual router, the current virtual router context is used.
- *ipAddress*—IP address to be used to reach the destination

Mode Global Configuration

l2tp disable calling-number-avp

Syntax [no] l2tp disable calling-number-avp

Release Information Command introduced before JunosE Release 7.1.0.

Description Prevents the E Series LAC from sending the Calling Number attribute value pair (AVP) in incoming-call-request (ICRQ) packets. The **no** version enables sending of the Calling Number AVP, the default setting.

Mode Global Configuration

l2tp disable challenge

Syntax [no] l2tp disable challenge

Release Information Command introduced before JunosE Release 7.1.0.

Description Disables the generation of local tunnel authentication challenges. The **no** version enables local challenge generation, which is the default setting.

Mode Global Configuration

l2tp drain

Syntax [no] l2tp drain

Release Information Command introduced before JunosE Release 7.1.0.

Description Prevents the creation of new destinations, tunnels, and sessions for the router. This command works in conjunction with the **l2tp shutdown** command. Both commands affect the status of the administrative state of L2TP on the router; the **l2tp drain** command sets the administrative state to drain. The **no** version allows the creation of new destinations, tunnels, and sessions for the router.

Mode Global Configuration

l2tp drain destination

Syntax [no] l2tp drain destination { *destinationName*
| [virtual-router *vrName*] ip *ipAddress* }

Release Information Command introduced before JunosE Release 7.1.0.

Description Prevents the creation of new tunnels and sessions at a destination. This command works in conjunction with the **l2tp shutdown destination** command. Both commands affect the status of the administrative state of L2TP for the destination; the **l2tp drain destination** command sets the administrative state to drain. The **no** version allows the creation of new tunnels and sessions at a destination.

Options
- *destinationName*—Name the router assigns to the LNS
- *vrName*—Name of the virtual router on which the destination exists
- *ipAddress*—IP address of the LNS

Mode Global Configuration

l2tp drain tunnel

Syntax [no] l2tp drain tunnel { *destinationName* |
[virtual-router *vrName*] ip *ipAddress tunnelName* }

Release Information Command introduced before JunosE Release 7.1.0.

Description Prevents the assignment of new sessions to a tunnel. This command works in conjunction with the **l2tp shutdown tunnel** command. Both commands affect the status of the administrative state of L2TP for the tunnel; the **l2tp drain tunnel** command sets the administrative state to drain. The **no** version allows the assignment of new sessions to a tunnel.

Options

- *destinationName*—Name the router assigns to the LNS
- *vrName*—Name of the virtual router on which the tunnel exists
- *ipAddress*—IP address of the LNS
- *tunnelName*—Name of the tunnel

Mode Global Configuration

l2tp ignore-receive-data-sequencing

Syntax [no] l2tp ignore-receive-data-sequencing

Release Information Command introduced before JunosE Release 7.1.0.

Description Suppresses sequence number checking for data packets received on all L2TP tunnels in the router. This setting affects only packets received on a tunnel, not packets sent on a tunnel. The L2TP LAC still inserts sequence numbers into data packets if the LAC receives packets from the LNS that contain sequence numbers. The **no** version restores the default, which causes the router to check the sequence numbers in data packets that it receives on L2TP tunnels.

NOTE: If you are using IP reassembly, we recommend that you set up the router to ignore sequence numbers in received data packets. Because IP reassembly may reorder L2TP packets, out-of-order packets may be dropped if sequence numbers are being used on L2TP data packets.

Mode Global Configuration

l2tp retransmission

Syntax l2tp retransmission *retries* [established | not-established]

no l2tp retransmission [*retries*] [established | not-established]

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets the number of retransmission retries, and allows you to apply the retry count to established and/or unestablished tunnels. If you do not include a keyword, the router applies the retry count to all tunnels. The **no** version resets the number of retransmissions to the default value, 5.

NOTE: If you perform a stateful SRP switchover on an LNS device, we recommend that you configure the maximum number of retransmission attempts as 10, although the default number of attempts is 5. This recommendation applies for all types of L2TP peer resynchronization methods configured for LNS devices.

Options

- *retries*—Number in the range 2–30
- established—Applies the retry count only to established tunnels
- not-established—Applies the retry count only to tunnels that are not established

Mode Global Configuration

l2tp shutdown

Syntax [no] l2tp shutdown

Release Information Command introduced before JunosE Release 7.1.0.

Description Closes all destinations, tunnels, and sessions and prevents the creation of new destinations, tunnels, and sessions for the router. This command works in conjunction with the **l2tp drain** command. Both commands affect the status of the administrative state of L2TP on the router; the **l2tp shutdown** command sets the administrative state to disabled. The **no** version enables the creation of new destinations, tunnels, and sessions for the router.

Mode Global Configuration

l2tp shutdown destination

Syntax [no] l2tp shutdown destination { *destinationName* |
[virtual-router *vrName*] ip *ipAddress* }

Release Information Command introduced before JunosE Release 7.1.0.

Description Closes all tunnels and sessions at a destination, and prevents the creation of new tunnels and sessions at that destination. This command works in conjunction with the **l2tp drain destination** command. Both commands affect the status of the administrative state of L2TP on the destination; the **l2tp shutdown destination** command sets the administrative state to disabled. The **no** version enables the creation of new tunnels and sessions at that destination.

Options

- *destinationName*—Name the router assigns to the LNS
- *vrName*—Name of the virtual router on which the destination exists
- *ipAddress*—IP address of the LNS

Mode Global Configuration

l2tp shutdown session

Syntax [no] l2tp shutdown session { *destinationName* |
[virtual-router *vrName*] ip *ipAddress sessionName* }

Release Information Command introduced before JunosE Release 7.1.0.

Description Closes a specific session. The **no** version has no effect because all L2TP sessions are dynamic and cannot be restarted after they have been shut down.

Options
- *destinationName*—Name that the router assigns to the LNS
- *vrName*—Name of the virtual router on which the destination exists
- *ipAddress*—IP address of the LNS
- *sessionName*—Name of the session

Mode Global Configuration

l2tp shutdown tunnel

Syntax [no] l2tp shutdown tunnel { *destinationName* |
[virtual-router *vrName*] ip *ipAddress tunnelName* }

Release Information Command introduced before JunosE Release 7.1.0.

Description Closes all sessions in a tunnel, and prevents the creation of new sessions in that tunnel. This command works in conjunction with the **l2tp drain tunnel** command. Both commands affect the status of the administrative state of L2TP on the tunnel; the **l2tp shutdown tunnel** command sets the administrative state to disabled. The **no** version enables the creation of new sessions in that tunnel.

Options

- *destinationName*—Name the router assigns to the LNS
- *vrName*—Name of the virtual router on which the tunnel exists
- *ipAddress*—IP address of the LNS
- *tunnelName*—Name of the tunnel

Mode Global Configuration

l2tp tunnel short-drain-timeout

Syntax l2tp tunnel short-drain-timeout [*timeOutValue*]

no l2tp tunnel short-drain-timeout

Release Information Command introduced in JunosE Release 7.1.0.

Description Configures the amount of time a disconnected LAC L2TP tunnel waits (the drain timeout) before restarting after a restart request is received. The **no** version restores the default setting.

Options

- *timeOutValue*—Short drain timeout in seconds, in the range 0–31; default value is 2 seconds

Mode Global Configuration

local host

Syntax local host *hostname*

no local host

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures an L2TP local hostname to be used with a remote host. The **no** version removes the local hostname from use with a remote host.

Options
- *hostname*—L2TP local hostname; string of up to 64 characters (no spaces)

Mode L2TP Destination Profile Host Configuration

local ip address

Syntax From L2TP Destination Profile Host Configuration mode:

local ip address *ipAddress*

no local ip address

From IPsec Transport Profile Configuration mode:

[no] local ip address *transportIpAddress*

From IPsec Tunnel Profile Configuration mode:

local ip address *transportIpAddress* { pre-share *keyString*
| pre-share-masked *maskedKeyString* }

no local ip address

Release Information Command introduced before JunosE Release 7.1.0.
IPsec Tunnel Profile Configuration mode added in JunosE Release 7.3.0.

Description From L2TP Destination Profile Host Configuration mode, configures a local IP address for use with a remote host. The **no** version removes the local IP address from use with a remote host.

From IPsec Transport Profile Configuration mode, specifies the local endpoint of the IPsec transport connection. It also enters Local IPsec Transport Profile Configuration mode. The **no** version deletes the local IP address.

From IPsec Tunnel Profile Configuration mode, specifies the given local IP address as a server address. The router continues to monitor UDP port 500 for incoming user login requests (that is, IKE source address negotiations). When using global preshared keys, consider the following points:

- Global preshared keys enable a group of users to share a single authentication key. Using a shared key for a group of users simplifies the administrative job of setting up keys. However, changing or removing a preshared key for one user (for security reasons) affects other users with the same key.
- Specific keys for individual users take precedence over global keys assigned to the same user. In other words, if a user has both an assigned specific key and a global key that user must use the specific key or authentication fails.
- Avoid specifying the same local endpoint and virtual router in the same profile. Local endpoint and virtual router values override each other. The last value set in the profile is the value used.

The **no** version causes the router to stop monitoring UDP port 500 for user requests and removes any preshared key associations with the local IP address.

Options

- *ipAddress*—IP address used in packets sent to the LAC
- *transportIpAddress*—Local endpoint for the IPsec transport connection
- *keyString*—Key value in ASCII format
- *maskedKeyString*—Key value in ascii format

Mode IPsec Transport Profile Configuration, IPsec Tunnel Profile Configuration, L2TP Destination Profile Host Configuration

max-sessions

Syntax For RADIUS:

max-sessions *sessionLimit*

no max-sessions

For AAA domain map and tunnel group tunnels:

max-sessions *maxSessionsPerTunnel*

{ no | default } max-sessions

For L2TP:

max-sessions *maxSessionsPerProfile*

{ no | default } max-sessions

Release Information Command introduced before JunosE Release 7.1.0.

Description For RADIUS, specifies the number of outstanding requests to a server. The **no** version reverts to the default value.

For AAA domain map, and tunnel group tunnels , sets the maximum sessions per tunnel. The **no** version disables the feature. The **default** version sets the value to zero.

For L2TP, sets the maximum sessions allowed for destination and host profiles by the LNS. The **no** and **default** versions disable the feature.

Options

- *sessionLimit*—Maximum number of outstanding requests to a specific server in the range from 10 through to the maximum value; default value is 255

  For information about the number of concurrent RADIUS requests that the router supports for authentication and accounting servers, see *JunosE Release Notes*, *Appendix A*, *System Maximums*.

- *maxSessionsPerTunnel*—Maximum number of sessions that can be configured on a tunnel in the range 0–4294967295; default value is zero

- *maxSessionsPerProfile*—Maximum number of sessions that can be established at the LNS for a destination or host profile; in the range from 1 through to a maximum of the chassis-wide limit; default value is the chassis-wide limit

  For information about the maximum number of L2TP sessions supported per chassis, see *JunosE Release Notes*, *Appendix A*, *System Maximums*.

Mode Domain Map Tunnel Configuration, L2TP Destination Profile Configuration, L2TP Destination Profile Host Configuration, RADIUS Configuration, Tunnel Group Tunnel Configuration, L2TP Destination Profile Sessions Limit Configuration, L2TP Destination Profile Host Sessions Limit Configuration

medium ipv4

Syntax medium ipv4

no medium

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the medium type of a tunnel to IPv4 (the only medium type currently supported). The **no** version restores the default value, ipv4.

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

password

Syntax Login password:

password [*encryptionType*] *passwordValue*

no password

L2TP tunnel password:

password *tunnelPassword*

no password

IP service profile password:

password *servicePassword*

no password

Local user database password:

password [*encryptionType*] *passwordValue*

no password

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures a password to be used at login on the console, a line or a range of lines. For L2TP, specifies the password for an AAA domain map or tunnel group tunnel. For IP service profiles, specifies the password for the profile. For the local authentication server feature, adds a password to a user entry in the local user database. If you enable password checking but do not configure a password, the system will not allow you to access virtual terminals. Specify a password in plain text (unencrypted) or cipher text (encrypted). In either case, the system stores the password as encrypted. The **no** version removes the password.

NOTE: To use an encrypted password, you must follow the procedure in *Creating Encrypted Passwords* in the *JunosE System Basics Configuration Guide* to obtain the encrypted password. You cannot create your own encrypted password; you must use a router-generated password or secret.

Options

- *encryptionType*—One of the following types:
  - 0—Unencrypted (the default)
  - 5—Secret

  - 7—Encrypted

- *passwordValue*—Character string that specifies the line password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 50 characters. The password checking is case sensitive.
- *tunnelPassword*—Password of up to 32 characters
- *servicePassword*—Password of up to 32 characters
- *encryptionType*—One of the following types:
  - 0—Unencrypted password (the default)
  - 8—Two-way encrypted password
- *passwordValue*—Character string that specifies the password. The string can contain any alphanumeric character, including spaces, up to 64 characters. Passwords are case sensitive.

Mode Domain Map Tunnel Configuration (for a tunnel password), IP Service Profile Configuration (for a service profile password), Line Configuration (for a login password), Local User Configuration (for a local user database password), Tunnel Group Tunnel Configuration (for a tunnel group tunnel password)

preference

Syntax preference *tunnelPreference*

no preference

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the preference value for an L2TP tunnel. The **no** version restores the default value, 2000.

Options
- *tunnelPreference*—Tunnel preference, in the range 0–2000; 0 is the highest preference

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

radius remote-circuit-id-delimiter

Syntax radius remote-circuit-id-delimiter *delimiter*

no radius remote-circuit-id-delimiter

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the delimiter character that sets off components in the PPPoE remote circuit ID value sent from a DSLAM and captured on the router. The **no** version restores the default delimiter character, #.

Options

- *delimiter*—Special character (for example, ! or %) to set off components in the PPPoE remote circuit ID value captured from a DSLAM; the default delimiter character is #

Mode Global Configuration

radius remote-circuit-id-format

Syntax radius remote-circuit-id-format { [nas-identifier] { agent-circuit-id | agent-remote-id | agent-circuit-id agent-remote-id } | dsl-forum-1 }

no radius remote-circuit-id format

Release Information Command introduced before JunosE Release 7.1.0.
dsl-forum-1 keyword added in JunosE Release 7.2.0.

Description Specifies the format of the PPPoE remote circuit ID value sent from a DSLAM and captured on the router. You can format the PPPoE remote circuit ID value to include either or both of the agent-circuit-ID (suboption 1) and agent-remote-id (suboption 2) suboptions of the DHCP relay agent information option (option 82) or the PPPoE intermediate agent tags, with or without the NAS-Identifier [32] RADIUS attribute. The **no** version restores the default format, agent-circuit-id.

Options

- nas-identifier—Formats the PPPoE remote circuit ID value to include the NAS-Identifier [32] RADIUS attribute with either or both of the agent-circuit-id and agent-remote-id suboptions. If you include the **nas-identifier** keyword, you must also include either or both of the **agent-circuit-id** and **agent-remote-id** keywords.
- agent-circuit-id—Formats the PPPoE remote circuit ID value to include only the agent-circuit-id suboption; this is the default format
- agent-remote-id—Formats the PPPoE remote circuit ID value to include only the agent-remote-id suboption
- agent-circuit-id agent-remote-id—Formats the PPPoE remote circuit ID value to include both the agent-circuit-id and agent-remote-id suboptions
- dsl-forum-1—Formats the PPPoE remote circuit ID value to append the agent-circuit-id suboption value to an interface specifier that is consistent with the recommended format in the DSL Forum Technical Report (TR)-101—Migration to Ethernet-Based DSL Aggregation (April 2006).

Mode Global Configuration

radius override calling-station-id remote-circuit-id

Syntax radius override calling-station-id remote-circuit-id

no radius override calling-station-id

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures RADIUS to override the standard use of the Calling-Station-Id [31] RADIUS attribute and instead use the PPPoE remote circuit ID transmitted from a DSLAM device. The **no** version restores the default Calling-Station-Id value, which is the telephone number from which the call originated.

Mode Global Configuration

radius connect-info-format

Syntax radius connect-info-format { l2tp-connect-speed | l2tp-connect-speed-rx-when-equal }

no radius connect-info-format

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the format and enables the generation of RADIUS attribute 77, Connect-Info, on the LNS. The format uses the received L2TP connect-speed AVPs that the LAC sends to the LNS. The **no** version restores the default, in which the LNS does not generate the Connect-Info attribute.

Options

- l2tp-connect-speed—Specifies that the Connect-Info attribute include only the RX speed when the RX speed is different from the TX speed and is greater than zero.
- l2tp-connect-speed-rx-when-equal—Specifies that the Connect-Info attribute always include the RX speed when the speed is greater than zero.

Mode Global Configuration

radius calling-station-format

Syntax radius calling-station-format { delimited | fixed-format [stacked] | fixed-format-adapter-embedded [stacked] | fixed-format-adapter-new-field [stacked] }

no radius calling-station-format

Release Information Command introduced before JunosE Release 7.1.0.
fixed-format-adapter-embedded and **fixed-format-adapter-new-field** keywords added in JunosE Release 8.1.0.
stacked keyword added in JunosE Release 9.3.0.

Description On a virtual router, specifies the format of RADIUS attribute 31, Calling-Station-Id, when the PPP user is terminated at the non-LNS E Series router. Depending on the keyword you use, the virtual router uses the specified format for each interface type, replacing variables in the format with their actual values for your configuration. The **no** version restores the default Calling-Station-Id format, **delimited**.

NOTE:

- Attribute 31, Calling-Station-Id, is used with Attribute 30, Called-Station-Id, in a standard way when the router is the LNS and the LAC is a dial-up LAC (not an E Series router). When the LNS receives the Calling-Station-Id and Called-Station-Id AVPs, the router includes the values as they are, with no format changes in the RADIUS messages.
- For subscribers connected over the LAG interface in DHCP standalone authenticate mode, the **radius override calling-station-id remote-circuit-id** command enables RADIUS to use the PPPoE remote circuit ID for the Calling-Station-Id attribute. By default, RADIUS uses a delimited format for the interface description. You cannot use this command to change the value of the Calling-Station-Id attribute.

Options

- delimited—Specifies that the RADIUS client uses the delimited format:
  - Format for ATM interfaces:
    delimiter systemName delimiter interfaceDescription delimiter VPI delimiter VCI delimiter
  - Format for Ethernet interfaces:
    delimiter systemName delimiter interfaceDescription delimiter VLAN

  Where *interfaceDescription* is one of the following items:

  - *port name*—The default setting
  - *VP description*—Appears if you use the **atm vp-description** command to assign a text description to an individual VP on an ATM interface

  - *VC description*—Appears if you use the **atm atm1483 description** command to assign a text description to VCs on an ATM 1483 subinterface and you use the **atm1483 export-subinterface-description** command to enable sending of VC interface descriptors to AAA

- fixed-format—Specifies that the RADIUS client uses a fixed format of up to 15 characters consisting of all ASCII fields:
  - Format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VPI* (3 bytes)
    VCI (5 bytes)
  - Format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VLAN* (8 bytes)
  - Format for serial interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) 0 (8 bytes)
  - In the case of PPP terminated from LNS, the Calling-Station-Id attribute value is based on the received L2TP calling number AVP
- fixed-format-adapter-embedded—Specifies that the RADIUS client uses a fixed format of up to 15 characters consisting of all ASCII fields with a 1-byte *slot* field, 1-byte *adapter* field, and 1-byte *port* field:
  - Format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte)
    VPI (3 bytes) *VCI* (5 bytes)
  - Format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte)
    VLAN (8 bytes)
  - Format for serial interfaces:
    systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte)
    0 (8 bytes)
  - For E120 routers and E320 routers, *adapter* is the number of the bay in which the I/O adapter (IOA) resides, either 0 (representing the right IOA bay on the E120 router and the upper IOA bay on the E320 router) or 1 (representing the left IOA bay on the E120 router or the lower IOA bay on the E320 router). For ERX7xx models, ERX14xx models, and ERX310 routers, *adapter* is always shown as 0.
  - Slot numbers 0 through 16 are shown as ASCII characters in the 1-byte slot field according to the following translation:

Slot Number	ASCII Character	Slot Number	ASCII Character
0	0	9	9
1	1	10	A
2	2	11	B

Slot Number	ASCII Character	Slot Number	ASCII Character
3	3	12	C
4	4	13	D
5	5	14	E
6	6	15	F
7	7	16	G
8	8	–	–

For example, slot 16 is shown as the ASCII character uppercase G.

- fixed-format-adapter-new-field—Specifies that the RADIUS client uses a fixed format of up to 17 characters consisting of all ASCII fields with a 2-byte *slot* field, 1-byte *adapter* field, and 2-byte *port* field:
  - Format for ATM interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *VPI* (3 bytes) *VCI* (5 bytes)
  - Format for Ethernet interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *VLAN* (8 bytes)
  - Format for serial interfaces:
    systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) 0 (8 bytes)
  - For E120 routers and E320 routers, *adapter* is the number of the bay in which the IOA resides, either 0 or 1. For ERX7xx models, ERX14xx models, and ERX310 routers, *adapter* is always shown as 0.
  - Slot numbers 0 through 16 are shown as integers in the 2-byte *slot* field.

NOTE: **You must use this field when you configure the format of the Calling-Station-ID attribute on routers that have line modules that support more than seven physical ports.**

- stacked—Includes a 4-byte stacked VLAN (S-VLAN ID) for Ethernet interfaces when the RADIUS client uses the fixed-format, fixed-format-adapter-embedded, or fixed-format-adapter-new-field format; by default, these formats do not include the S-VLAN ID unless you specify the optional **stacked** keyword; If you include the stacked keyword, the S-VLAN ID is displayed in decimal format in the range 0–4095
  - Format for Ethernet interfaces that use **fixed-format**:

systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)

- Format for Ethernet interfaces that use **fixed-format-adapter-embedded**: *systemName* (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
- Format for Ethernet interfaces that use **fixed-format-adapter-new-field**: *systemName* (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *S-VLAN* (4 bytes) *VLAN* (4 bytes)

NOTE:

- The use of the **stacked** keyword is not supported for VLAN subinterfaces based on agent-circuit-identifier information, otherwise known as ACI VLANs. When you issue the **radius calling-station-format fixed-format stacked**, **radius calling-station-format fixed-format-adapter-embedded stacked**, or **radius calling-station-format fixed-format-adapter-new-field stacked** command for an ACI VLAN, the values that appear in the 4-byte S-VLAN ID and 4-byte VLAN ID fields are incorrect.
- The S-VLAN ID field in the Calling-Station-Id [31] attribute is set to 0 (zero) under the following conditions:
  - You do not specify the optional **stacked** keyword.
  - You specify the optional **stacked** keyword but the Ethernet interface does not have an S-VLAN ID.

Mode Global Configuration

remote host

Syntax [no] remote host { *hostname* | default }

Release Information Command introduced before JunosE Release 7.1.0.

Description Defines an L2TP host profile. Accesses the L2TP Destination Profile Host Configuration mode. The **no** version removes an L2TP host profile.

Options
- *hostname*—Name the LAC must supply in the hostname AVP of the receive SCCRQ; can be up to 64 characters in length (no spaces)
- default—Allows the LAC to use any hostname in the hostname AVP

Mode L2TP Destination Profile Configuration

router-name

Syntax router-name *vrName*

no router-name [*vrName*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Maps a virtual router to a user domain name. The **no** version deletes the router name parameter, and the router defaults to the default virtual router.

NOTE: This command is deprecated and might be removed completely in a future release. The functionality provided by this command has been replaced by the **auth-router-name** and **ip-router-name** commands.

Options

- *vrName*—Name of the virtual router to map to the user domain name

Mode Domain Map Configuration, Tunnel Group Tunnel Configuration

server-name

Syntax server-name *serverName*

no server-name

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the hostname expected from the L2TP LNS when you set up a tunnel. The **no** version removes the server name.

Options
- *serverName*—Hostname; can be up to 64 characters in length (no spaces)

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

session-out-of-resource-result-code-override

Syntax [no] session-out-of-resource-result-code-override

Release Information Command introduced in JunosE Release 9.2.0.

Description Overrides out-of-resource result codes 4 [Call failed due to lack of appropriate facilities being available (temporary condition)] and 5 [Call failed due to lack of appropriate facilities being available (permanent condition)] with code 2 (Call disconnected for the reason indicated in error code) on a router configured as an LNS. The **no** version halts the overriding of codes 4 and 5.

Mode L2TP Destination Profile Host Configuration

source-address

Syntax source-address *sourceAddress*

no source-address

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies a source IP address for the LAC tunnel endpoint. The **no** version removes the source address.

Options
- *sourceAddress*—Address of the local tunnel endpoint (the LAC); can be up to 32 characters (no spaces)

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

tunnel

Syntax [no] tunnel *tag*

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies an L2TP tunnel and changes the mode to Domain Map Tunnel Configuration. In Domain Map Tunnel Configuration mode, you can set the attributes of the tunnel. The **no** version deletes the L2TP tunnel configuration from the router.

From Tunnel Group Configuration mode, adds up to 31 tunnel definitions to the L2TP tunnel group and changes the mode to Tunnel Group Tunnel Configuration mode. In Tunnel Group Tunnel Configuration mode, you can set tunnel attributes. The **no** version deletes the L2TP tunnel group configuration from the router.

Options
- *tag*—Number in the range 1–31

Mode Domain Map Configuration, Tunnel Group Configuration

tunnel group

Syntax tunnel group *tunnelGroupName*

no tunnel group

Release Information Command introduced before JunosE Release 7.1.0.

Description Assigns the specified tunnel group to the domain map. The **no** version deletes the tunnel group.

NOTE: By default, no tunnel group is assigned to the domain map. You can assign a tunnel group to the domain map only if tunnels are not currently defined for the domain map in Domain Map Tunnel mode.

Options

- *tunnelGroupName*—String of up to 64 characters (no spaces)

Mode Domain Map Configuration

type

Syntax To configure the RTR operation:

[no] type *rtrType* protocol ipIcmpEcho *destination*
[source-ipaddr *srcAddr* | source *interfaceType interfaceSpecifier*]

To specify the L2TP tunnel type:

type *tunnelType*

no type

Release Information Command introduced before JunosE Release 7.1.0.

Description From RTR Configuration mode, configures an RTR operation. The **no** version removes the configured type from the operation and resets all configuration for an RTR index.

NOTE: **You must configure the operation's type before you can configure any other characteristics of the operation.**

From Domain Map Configuration and Tunnel Group Tunnel Configuration modes, specifies the L2TP tunnel type (RADIUS attribute 64, Tunnel-Type).

Options

- *rtrType*—One of the following types of operation:
  - echo—Performs end-to-end operation only
  - pathEcho—Discovers a path to the destination and echoes each device on the path
- *destination*—IP address or an IP hostname or domain name
- *srcAddr*—Source IP address
- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
- *tunnelType*—L2TP tunnel type

Mode Domain Map Configuration, RTR Configuration, Tunnel Group Tunnel Configuration

tunnel password

Syntax tunnel password *tunnelPassword*

no tunnel password

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures a password for the L2TP tunnel. The **no** version removes the password.

Options
- *tunnelPassword*—Password used for challenge response to the tunnel peer; in the domain map, it is used only by the LAC

Mode L2TP Destination Profile Host Configuration

virtual-router

Syntax virtual-router *vrName* | :*vrfName* | *vrName*:*vrfName*

no virtual-router *vrName* [wait-for-completion [*waitSeconds*]]

Release Information Command introduced before JunosE Release 7.1.0.

Description Creates a virtual router or accesses the context of a previously created virtual router or a VRF. The **no** version deletes the virtual router, and the router defaults to the default virtual router. Issuing a **no** version that specifies an existing VRF only displays the error message: " Cannot delete a VRF with this command." You must use the **no ip vrf** command to remove a VRF.

NOTE: In Domain Map Configuration mode, the **virtual-router** command has been replaced by the router-name command and may be removed completely from Domain Map Configuration mode in a future release.

Options

- *vrName*—Name of the virtual router; a string of 1–32 alphanumeric characters
- :*vrfName*—Name of a VRF in the current VR context; a string of 1–32 alphanumeric characters
- *vrName*:*vrfName*—Name of a VRF in the context of a VR other than the current VR
- wait-for-completion—Specifies (in the absence of *waitSeconds*) that the CLI waits for completion of the **no** version operation before it returns a prompt, regardless of how long that takes
- *waitSeconds*—Number of seconds, in the range 1–64000, that the CLI waits before it returns a prompt, regardless of whether the **no** version operation has been completed

Mode Global Configuration, Privileged Exec

PART 3

Administration

CHAPTER 15

Verifying Domain Maps and L2TP Tunnels with AAA

Monitoring the Mapping for User Domains and Virtual Routers with AAA

Purpose Display the mapping between user domains and virtual routers.

Action To display the mapping between user domains and virtual routers:

```
host1#show aaa domain-map

Domain: lac-tunnel; router-name: lac; ipv6-router-name: default
Tunnel                 Tunnel   Tunnel   Tunnel    Tunnel
 Tag     Tunnel Peer   Source    Type    Medium   Password    Tunnel Id
------   -----------   ------   ------   ------   --------   -----------
5        192.168.1.1   <null>   l2tp     ipv4     welcome    lac-tunnel

                       Tunnel                Tunnel
Tunnel     Tunnel      Server     Tunnel       Max
 Tag     Client Name    Name    Preference   Sessions     Tunnel RWS
------   -----------   ------   ----------   --------   --------------
5        lac           boston   5            0          4

                                                 Tunnel
         Tunnel     Tunnel      Tunnel        Tx
Tunnel   Virtual   Failover     Switch      Speed
 Tag     Router     Resync     Profile      Method
------   -------   --------   ---------    ------
5        <null>    <null>      denver      qos
```

Meaning Table 13 on page 137 lists the **show aaa domain-map** command output fields.

Table 13: show aaa domain-map Output Fields

Field Name	Field Description
Domain	Name of the domain
router-name	Virtual router to which user domain name is mapped

Table 13: show aaa domain-map Output Fields *(continued)*

Field Name	Field Description
router-mask	IPv4 mask of the local interface
tunnel-group	Name of the tunnel group assigned to the domain map
ipv6-router-name	IPv6 virtual router to which user domain name is mapped
local-interface	Interface information to use on the local (E Series) side of the subscriber's interface
ipv6-local-interface	IPv6 interface information to use on the local (E Series) side of the subscriber's interface
poolname	Local address pool from which the router allocates addresses for this domain
IP hint	IP hint is enabled
strip-domain	Strip domain is enabled
override-username	Single username used for all users from a domain in place of the values received from the remote client
override-password	Single password used for all users from a domain in place of the values received from the remote client
Tunnel Tag	Tag that identifies the tunnel
Tunnel Peer	Destination address of the tunnel
Tunnel Source	Source address of the tunnel
Tunnel Type	L2TP
Tunnel Medium	Type of medium for the tunnel; only IPv4 is supported
Tunnel Password	Password for the tunnel
Tunnel Id	ID of the tunnel
Tunnel Client Name	Host name that the LAC sends to the LNS when communicating to the LNS about the tunnel
Tunnel Server Name	Host name expected from the peer (the LNS) when during tunnel startup
Tunnel Preference	Preference level for the tunnel

Table 13: show aaa domain-map Output Fields *(continued)*

Field Name	Field Description
Tunnel Max Sessions	Maximum number of sessions allowed on a tunnel
Tunnel RWS	L2TP receive window size (RWS) for a tunnel on the LAC; displays either the configured value or the default behavior, which is indicated by system chooses
Tunnel Virtual Router	Name of the virtual router to map to the user domain name
Tunnel Failover Resync	L2TP peer resynchronization method
Field descriptions	The actual fields displayed depend on your configuration
Tunnel Switch Profile	Name of the L2TP tunnel switch profile
Tunnel Tx Speed Method	Method that the router uses to calculate the transmit connect speed of the subscriber's access interface: static layer2, dynamic layer2, qos, actual, not set

Related Documentation

- show aaa domain-map on page 180

Monitoring Configuration of Tunnel Parameters with AAA

Purpose Display configuration of tunnel parameters used for tunnel definitions.

Action To display the configuration of tunnel parameters used for tunnel definitions:

```
host1#show aaa tunnel-parameters
Tunnel password is 3&92k%b#q4
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel switch profile is boston
Tunnel tx-connect-speed-method is qos
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
Tunnel assignmentId format is assignmentId
Tunnel calling number format is fixed (stacked)
 Tunnel calling number format fallback is fixed
```

Meaning Table 14 on page 139 lists the **show aaa tunnel-parameters** command output fields.

Table 14: show aaa tunnel-parameters Output Fields

Field Name	Field Description
Tunnel password	Default tunnel password

Table 14: show aaa tunnel-parameters Output Fields *(continued)*

Field Name	Field Description
Tunnel client-name	Hostname that the LAC sends to the LNS when communicating about the tunnel
Tunnel nas-port-method	Default NAS port type
Tunnel switch profile is	Name of the default L2TP tunnel switch profile
Tunnel tx-connect-speed-method is	Method that the router uses to calculate the transmit connect speed of the subscriber's access interface: static layer2, dynamic layer2, qos, actual, not set
Tunnel nas-port ignore	Whether the router uses the tunnel peer's NAS-Port [5] attribute; enabled or disabled
Tunnel nas-port-type ignore	Whether the router uses the tunnel peer's NAS-Port-Type [61] attribute; enabled or disabled
Tunnel assignmentId format	Value of the tunnel assignment ID that is passed to PPP/L2TP
Tunnel calling number format	Format configured for L2TP Calling Number AVP 22 generated by the LAC
Tunnel calling number format fallback	Fallback format configured for L2TP Calling Number AVP 22 generated by the LAC

Related Documentation

- show aaa tunnel-parameters on page 182

Monitoring Configured Tunnel Groups with AAA

Purpose Display the currently configured tunnel groups.

Action To display information about currently configured tunnel groups:

```
host1#show aaa tunnel-group

Tunnel Group: boston
Tunnel                  Tunnel   Tunnel   Tunnel    Tunnel
 Tag     Tunnel Peer    Source    Type    Medium   Password    Tunnel Id
------   -----------   ------   ------   ------   --------   -----------
3        192.168.1.1   <null>   l2tp     ipv4     msn        <null>

                       Tunnel                Tunnel
Tunnel     Tunnel      Server     Tunnel      Max
 Tag     Client Name    Name    Preference   Sessions     Tunnel RWS
------   -----------   ------   ----------   --------   --------------
3        msn.del.com   <null>   2000         0          4

                                           Tunnel
         Tunnel     Tunnel      Tunnel       Tx
Tunnel   Virtual   Failover     Switch     Speed
```

```
 Tag     Router     Resync     Profile     Method
------   -------   --------   ---------    ------
3        <null>    <null>      sanjose     qos
```

Meaning Table 15 on page 141 lists the **show aaa tunnel-group** command output fields.

Table 15: show aaa tunnel-group Output Fields

Field Name	Field Description
Domain	Name of the domain
router-name	Virtual router to which user domain name is mapped
router-mask	IPv4 mask of the local interface
tunnel-group	Name of the tunnel group assigned to the domain map
ipv6-router-name	IPv6 virtual router to which user domain name is mapped
local-interface	Interface information to use on the local (E Series) side of the subscriber's interface
ipv6-local-interface	IPv6 interface information to use on the local (E Series) side of the subscriber's interface
poolname	Local address pool from which the router allocates addresses for this domain
IP hint	IP hint is enabled
strip-domain	Strip domain is enabled
override-username	Single username used for all users from a domain in place of the values received from the remote client
override-password	Single password used for all users from a domain in place of the values received from the remote client
Tunnel Tag	Tag that identifies the tunnel
Tunnel Peer	Destination address of the tunnel
Tunnel Source	Source address of the tunnel
Tunnel Type	L2TP
Tunnel Medium	Type of medium for the tunnel; only IPv4 is supported
Tunnel Password	Password for the tunnel

Table 15: show aaa tunnel-group Output Fields *(continued)*

Field Name	Field Description
Tunnel Id	ID of the tunnel
Tunnel Client Name	Host name that the LAC sends to the LNS when communicating to the LNS about the tunnel
Tunnel Server Name	Host name expected from the peer (the LNS) when during tunnel startup
Tunnel Preference	Preference level for the tunnel
Tunnel Max Sessions	Maximum number of sessions allowed on a tunnel
Tunnel RWS	L2TP receive window size (RWS) for a tunnel on the LAC; displays either the configured value or the default behavior, which is indicated by system chooses
Tunnel Virtual Router	Name of the virtual router to map to the user domain name
Tunnel Failover Resync	L2TP peer resynchronization method
Field descriptions	The actual fields displayed depend on your configuration
Tunnel Switch Profile	Name of the L2TP tunnel switch profile
Tunnel Tx Speed Method	Method that the router uses to calculate the transmit connect speed of the subscriber's access interface: static layer2, dynamic layer2, qos, actual, not set

Related Documentation

- The information displayed is almost identical to the tunnel information displayed using the **show aaa domain-map** command. See Monitoring the Mapping for User Domains and Virtual Routers with AAA on page 137.
- show aaa tunnel-group on page 181

CHAPTER 16

Verifying the L2TP Tunnel Aggregated Settings

Monitoring Global Configuration Status on E Series Routers

Purpose Display the global configuration and status for L2TP on E Series routers, including switched sessions.

Action To display the global configuration and status for L2TP on E Series routers, including switched sessions:

```
host1#show l2tp
Configuration
  L2TP administrative state is enabled
  Dynamic interface destruct timeout is 600 seconds
  Data packet checksums are disabled
  Receive data sequencing is not ignored
  Tunnel switching is disabled
  Retransmission retries for established tunnels is 5
  Retransmission retries for not-established tunnels is 5
  Tunnel idle timeout is 60 seconds
  Failover within a preference level is disabled
  Weighted load balancing is disabled
  Tunnel authentication challenge is enabled
  Calling number avp is enabled
  Reject remote transmit address change is enabled for ip address
  Ignore remote transmit address change is disabled
  Disconnect-cause avp generation is enabled
  Default receive window size is system chooses
  Rx speed avp when equal is enabled
  Destination lockout timeout is 300 seconds
  Destination lockout test is disabled
  Failover resync is silent-failover
Sub-interfaces      total      active     failed     auth-errors
  Destinations      0          0          0          n/a
  Tunnels           0          0          0          0
  Sessions          0          0          0          n/a
  Switched-sessions 0          0          0          n/a
```

Meaning Table 16 on page 144 lists the **show l2tp** command output fields.

Table 16: show l2tp Output Fields

Field Name	Field Description
Configuration	Configuration and status for L2TP on E Series routers, including switched sessions
L2TP administrative state	Status of L2TP on the router; enabled or disabled
Dynamic interface destruct timeout	Number of seconds that the router maintains dynamic destinations, tunnels, and sessions after they have terminated
Data packet checksums	Status of checking data integrity via UDP; enabled or disabled
Receive data sequencing	Whether the router processes or ignores sequence numbers in incoming data packets
Tunnel switching	Enabled or disabled
Retransmission retries for established tunnels	Number of retries configured for established tunnels
Retransmission retries for not-established tunnels	Number of retries configured for tunnels not established
Tunnel idle timeout	Length of the tunnel idle timeout, in seconds
Failover within a preference level	Enabled or disabled
Weighted load balancing	Enabled or disabled
Tunnel authentication challenge	Enabled or disabled
Calling number avp	Whether the E Series LAC sends Calling-Station-Id and Called-Station-Id AVPs in ICRQ packets, enabled or disabled
Reject remote transmit address change	Enabled or disabled for IP address, UDP port, or both
Ignore remote transmit address change	Enabled or disabled for IP address, UDP port, or both
Disconnect-cause avp generation	Enabled or disabled
Default receive window size	Default L2TP RWS for a tunnel on both the LAC and the LNS; displays either the configured value or the default behavior, indicated by system chooses
Rx speed avp when equal	Enabled or disabled

Table 16: show l2tp Output Fields *(continued)*

Field Name	Field Description
Destination lockout timeout	Number of seconds that L2TP destinations remain in the lockout state after they become unavailable
Destination lockout test	Status of the L2TP destination lockout test, enabled or disabled
Failover resync	Global L2TP peer resynchronization configuration
Sub-interfaces	Sub-interface information about L2TP
total	Number of destinations, tunnels, and sessions that the router created
active	Number of operational destinations, tunnels, and sessions
failed	Number of requests that did not reach an operational state
auth-errors	Number of requests that failed because the tunnel password was invalid

Related Documentation

- show l2tp on page 183

CHAPTER 17

Monitoring L2TP Destination Settings

Monitoring Detailed Configuration Information for Specified Destinations

Purpose Display detailed configuration information about specified destinations.

Action To display detailed configuration information about specified destinations:

To display information about a specific destination:

```
host1#show l2tp destination ip 172.31.1.98
L2TP destination 1 is Up with 5 active tunnels and 64 active sessions
```

To display information about all destinations:

```
host1#show l2tp destination detail 1
L2TP destination 1 is Up with 5 active tunnels and 64 active sessions
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Destination address
  Transport ipUdp
  Virtual router default
  Local address 192.168.1.230, peer address 172.31.1.98
Destination status
  Effective administrative state is enabled
Sub-interfaces total active failed auth-errors
  Tunnels      5     5      0      0
  Sessions     64    64     0      n/a
Statistics    packets      octets       discards   errors
  Control rx  69           3251          2          0
  Control tx  195          23939         0          0
  Data rx     68383456     68383456      0          0
  Data tx     68383456     68383456       0         0
```

Meaning Table 17 on page 148 lists the **show l2tp destination** command output fields.

Table 17: show l2tp destination Output Fields

Field Name	Field Description
Configuration	Configured status of the destination
Administrative state	Administrative status of the destination: • enabled—No restrictions on creation and operation of sessions and tunnels for this destination • disabled—Router disabled existing sessions and tunnels and will not create new sessions or tunnels for this destination • drain—Router will not create new sessions or tunnels for this destination
SNMP traps	Whether or not the router sends traps to SNMP for operational state changes
Destination address	Address information for the specified destination
Transport	Method used to transfer traffic
Virtual	Name of the virtual router on which the tunnel is configured
Local and peer addresses	Addresses of the local and remote interfaces
Destination status	Effective administrative state—The more restrictive of the router and destination administrative states. This setting, rather than the administrative state of the destination, determines whether the router can create new sessions or tunnels and whether the sessions or tunnels are disabled for this destination.
Sub-interfaces	Sub-interface information about the L2TP destination
total	Number of sessions or tunnels that the router created for this destination
active	Number of operational sessions or tunnels for this destination
failed	Number of requests that did not reach an operational state for this destination
auth-errors	Number of requests that failed because the tunnel password was invalid for this destination
Statistics	Information about the traffic sent and received

Related Documentation

- show l2tp destination on page 184

Monitoring Configured and Operational Status of all Destinations

Purpose Display summary of the configured and operational status of all L2TP destinations.

Action To display a summary of the configured and operational status of all L2TP destinations.:

```
host1#show l2tp destination summary
Administrative status    enabled    drain      disabled
                         0          0          0
Operational status       up         down       lower-down not-present
                         0          0          0          0
```

Meaning Table 18 on page 149 lists the **show l2tp destination summary** command output fields.

Table 18: show l2tp destination summary Output Fields

Field Name	Field Description
Administrative status	Administrative status of the L2TP destination: • enabled—No restrictions on creation and operation of sessions and tunnels for this destination • drain—Router will not create new sessions or tunnels for this destination • disabled—Router disabled existing sessions and tunnels and will not create new sessions or tunnels for this destination
Operational status	Operational status of the L2TP destination: • up—Destination is available for tunnels • down—Destination is not available for tunnels • lower-down—Underlying transport is unavailable; for example, you removed the virtual router • not-present—Hardware supporting the destination is unavailable; for example, you removed a required line module

Related Documentation
- show l2tp destination on page 184

Monitoring Locked Out Destinations

Purpose Display information about the L2TP destinations that are currently locked out.

Action To display information about the L2TP destinations that are currently locked out:

```
host1#show l2tp destination lockout
L2TP destination 36 is waiting for lockout timeout (45 seconds remaining)
L2TP destination 54 is waiting for lockout test start
L2TP destination 76 is waiting for lockout test complete
3 L2TP lockout destinations found
```

Meaning Table 19 on page 150 lists the **show l2tp destination lockout** command output fields.

Table 19: show l2tp destination lockout Output Fields

Field Name	Field Description
L2TP destination waiting	Name of destination and its lockout status. The status indicates whether the destination is waiting for the lockout timeout to expire (and how much time is left), or waiting for the lockout test to start or finish
L2TP lockout destinations found	Number of destinations that are currently in lockout state

Related Documentation

- show l2tp destination lockout on page 185

Monitoring Configured L2TP Destination Profiles or Host Profiles

Purpose

Display either a list of configured Layer 2 Tunneling Protocol (L2TP) destination profiles or the host profiles defined in a particular profile.

If a nondefault L2TP receive window size (RWS) is configured for a particular host profile, the command displays the RWS setting as an attribute of that host profile.

Action

To display either a list of configured L2TP destination profiles or the host profiles defined in a particular profile:

```
host1#show l2tp destination profile
L2TP destination profile westford
1 L2TP destination profile found
```

If a nondefault L2TP RWS is configured for a particular host profile, to display the RWS setting as an attribute of that host profile:

```
host1#show l2tp destination profile westford
L2TP destination profile westford
Configuration
  Destination address
    Transport ipUdp
    Virtual router lns
    Peer address 192.168.1.99
  Destination profile maximum sessions is 5000
Current session count in group-A is 14, max-sessions configured is 3400
Current session count in group-B is 2, max-sessions configured is 4600
Statistics
  Destination profile current session count is 30
Host profile attributes
  Remote host is remhost22.xyz.com
    Configuration
      Tunnel password is 23erf5
      Interface profile is ebcints
      Bundled group id is 1
      Bundled group id override is enabled
      Maximum sessions is 400
      Failover resync is failover-protocol
      Sessions-limit-group is group-A
    Statistics
      Current session count is 14
```

```
  Remote host is asciitext
    Configuration
      Bundled group id is 0
      Tunnel password is 222
      Interface profile is ascints
      Default upper binding type mlppp
      Maximum sessions is 250
      Failover resync is failover-protocol
      Sessions-limit-group is group-B
  Statistics
      Current session count is 2
  Remote host is mexico
    Configuration
      Local ip address is 10.10.2.2
      Proxy lcp is disabled
      Proxy authenticate is enabled
      mlppp upper binding type
      Disconnect-cause avp is enabled
      Receive window size is 4
      Maximum sessions is 500
      Failover resync is failover-protocol
    Statistics
      Current session count is 14
  Remote host is LAC
    Configuration
      Tunnel password is TunnelPass
      Local host name is LNS
      Local ip address is 46.1.1.2
      Disconnect-cause avp is enabled
      Tunnels are single-shot
      Override out-of-resource-result-code is enabled
    Statistics
      Current session count is 0
5 L2TP host profiles found
```

Meaning Table 20 on page 151 lists the **show l2tp destination profile** command output fields.

Table 20: show l2tp destination profile Output Fields

Field Name	Field Description
Transport	Method used to transfer traffic
Virtual router	Name of the virtual router
Peer address	IP address of the L2TP access concentrator (LAC)
Destination profile maximum sessions	Maximum number of sessions allowed for the destination profile
Current session count in group-A	Number of current sessions in group-A
Current session count in group-B	Number of current sessions in group-B
Destination profile current session count	Number of current sessions for the destination profile

Table 20: show l2tp destination profile Output Fields *(continued)*

Field Name	Field Description
Host profile attributes	Host profile attributes of the L2TP destination
Remote host	Name of the remote host
Local host name	Name of the local host
Local ip address	IP address of the local host
Bundled group id	Identifier for bundled sessions
Bundled group id override	Status of the bundled group ID override: enabled or disabled
Tunnel password	Password for the tunnel
Interface profile	Name of the host profile
Default upper binding type	The default upper binding type: mlpp
Proxy lcp	Status of the proxy LCP for the remote host
mlppp upper binding type	Default upper binding type
Proxy authenticate	The status of the proxy authentication: enabled or disabled
Disconnect-cause avp	Status of the disconnect-cause attribute-value pair (AVP): enabled or disabled
Tunnels are single-shot	Indicates that single-shot tunnels are configured for this host profile
Receive window size	Number of packets that the peer can transmit without receiving an acknowledgment from the router
Maximum sessions	Maximum number of sessions allowed for the host profile
Failover resync	L2TP peer resynchronization method for the host profile
Override out-of-resource-result-code	State of the out-of-resource-result-code override: enabled or disabled
Current session count	Number of current sessions for the host profile
Sessions-limit-group	Name of the sessions limit group

Related Documentation

- *Configuring an L2TP Destination Profile to Enable IPsec Support for L2TP Tunnels*
- *Configuring Single-Shot L2TP/IPsec Tunnels*
- show l2tp destination profile on page 186

CHAPTER 18

Viewing the Disconnect Cause-Codes for PPP Sessions

Monitoring Statistics on the Cause of a Session Disconnection

Purpose Display statistics for all information the LAC receives from an LNS about the cause of an L2TP session disconnection.

Action To display statistics for all information the LAC receives from an LNS about the cause of an L2TP session disconnection.

```
host1# show l2tp received-disconnect-cause-summary
Disconnect Cause (Code)                          Global     Peer       Local
------------------------------------------------ ---------- ---------- ----------
no info (0)                                      0          0          0
admin disconnect (1)                             0          0          0
renegotiation disabled (2)                       0          0          0
normal disconnect (3)                            0          0          0
compulsory encryption refused (4)                0          0          0
lcp failed to converge (5)                       0          0          0
lcp peer silent (6)                              0          0          0
lcp magic number error (7)                       0          0          0
lcp keepalive failure (8)                        0          0          0
lcp mlppp endpoint discriminator mismatch (9)    0          0          0
lcp mlppp peer mrru not valid (10)               0          0          0
lcp mlppp peer ssn invalid (11)                  0          0          0
lcp callback refused (12)                        0          0          0
authenticate timed out (13)                      0          0          0
authenticate mlppp name mismatch (14)            0          0          0
authenticate protocol refused (15)               0          0          0
authenticate failure (16)                        0          0          0
ncp no negotiation completed (17)                0          0          0
ncp no ncps available (18)                       0          0          0
ncp addresses failed to converge (19)            0          0          0
ncp negotiation inhibited (20)                   0          0          0
```

Meaning Table 21 on page 156 lists the **show l2tp received-disconnect-cause-summary** command details.

Table 21: show l2tp received-disconnect-cause-summary Output Fields

Field Name	Field Description
show l2tp received-disconnect-cause-summary	Display statistics for all information the LAC receives from an LNS about the cause of an L2TP session disconnection.

Related Documentation

- show l2tp received-disconnect-cause-summary on page 187

CHAPTER 19

Viewing the Configured L2TP Session Details

Monitoring Detailed Configuration Information about Specified Sessions

Purpose Display detailed configuration information about specified sessions.

Action To display detailed configuration information about specified sessions:

To display L2TP session:

```
host1#show l2tp session
L2TP session 1/1/1 is Up
1 L2TP session found
```

To display L2TP session details:

```
host1#show l2tp session detail
L2TP session 1/1/1 is Up
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Session status
  Effective administrative state is enabled
  State is established
  Local session id is 25959, peer session id is 2
Statistics packets octets discards errors
  Data rx  7       237    1        0
  Data tx  6       160    0        0

Session operational configuration
  User name is 't1.s1@local'
  Tunneling PPP interface atm 0/0.1
  Call type is lacIncoming
  Call serial number is 0
  Bearer type is none
  Framing type is none
  Proxy LCP was provided
  Authentication method was chap
  Tunnel switch profile is chicago
```

Meaning Table 22 on page 158 lists the **show l2tp session** command output fields.

Table 22: show l2tp session Output Fields

Field Name	Field Description
Configuration	Configured status of the session
Administrative state	Administrative status of the destination: • enabled—No restrictions on the operation of this session • disabled—Router terminated this session
SNMP traps	Whether or not the router sends traps to Simple Network Management Protocol (SNMP) for operational state changes
Session status	Session status of the destination
Effective administrative state	Most restrictive of the following administrative states: router, destination, tunnel, and session. This setting, rather than the administrative state of the session, determines whether the router can maintain this session or not.
State	Status of the session: idle, connecting, established, or disconnecting
Local and peer session id	Names the router uses to identify the session locally and remotely
Statistics	Information about the traffic for this session
Session operational configuration	Information received from the peer when the session was created

Related Documentation

- show l2tp session on page 192

Monitoring Configured and Operational Summary Status

Purpose Display a summary of the configured and operational status of all L2TP sessions.

Action To display a summary of the configured and operational status of all L2TP sessions:

```
host1#show l2tp session summary
Administrative status  enabled   disabled
                       64        0
Operational status     up        down   lower-down   not-present
                       64        0      0            0
```

Meaning Table 23 on page 159 lists the **show l2tp session summary** command output fields.

Table 23: show l2tp session summary Output Fields

Field Name	Field Description
Administrative status:	Administrative status of the session: • enabled—No restrictions on the creation of sessions • disabled—Router disabled these sessions
Operational status:	Operational status of the session: • up—Session is available • down—Session is unavailable • lower-down—Session is unavailable because the tunnel supporting it is inaccessible • not-present—Session is unavailable because the hardware (such as a line module) supporting it is inaccessible

Related Documentation

- show l2tp session on page 192 summary

CHAPTER 20

Viewing L2TP Switch-Profiles

Monitoring Configured Switch Profiles on Router

Purpose Display information about the L2TP switch profiles configured on the router.

Action To display only the names of the L2TP tunnel switch profiles configured on the router:

```
host1#show l2tp switch-profile
L2TP tunnel switch profile concord
L2TP tunnel switch profile myProfile
2 L2TP tunnel switch profiles found
```

To display information about the settings in a particular L2TP tunnel switch profile:

```
host1#show l2tp switch-profile concord
L2TP tunnel switch profile concord
  AVP bearer type action is relay
  AVP calling number action is relay
  AVP Cisco nas port info action is relay
```

Meaning Table 24 on page 161 lists the **show l2tp switch-profile** command output fields.

Table 24: show l2tp switch-profile Output Fields

Field Name	Field Description
L2TP tunnel switch profile	Name of the L2TP tunnel switch profile
AVP *actionType* action is	Indicates the tunnel switching behavior or action type (for example, relay) configured for the specified L2TP AVP type

Related Documentation

- show l2tp switch-profile on page 193

CHAPTER 21

Monitoring L2TP Tunnel Settings

Monitoring Detailed Configuration Information about Specified Tunnels

Purpose Display detailed configuration information about specified tunnels.

Action To display detailed configuration information about specified tunnel by IP address:

NOTE: For L2TP tunnels configured with output IPv4 or IPv6 policy lists, the output of the **show ip interface tunnel** *l2tp:tunnel-name* and the **show ipv6 interface tunnel** *l2tp:tunnel-name* commands display only the forwarded packets and bytes fields, and the dropped packets and bytes fields in the rate-limit-profile section for policies with hierarchical parent groups under the IP policy output or IPv6 policy output headings, respectively, when scheduler profile–based computation of service session accounting is enabled. In such a case, the committed, conformed, exceeded, saturated, and unconditional packets and bytes fields are not displayed in the rate-limit-profile section in the output of these commands for policies with hierarchical parent groups.

```
host1#show l2tp tunnel virtual router default ip 172.31.1.98
L2TP tunnel 1/xyz is Up with 13 active sessions
L2TP tunnel 1/aol.com is Up with 13 active sessions
L2TP tunnel 1/isp.com is Up with 13 active sessions
L2TP tunnel 1/msn.com is Up with 13 active sessions
L2TP tunnel 1/mv.com is Up with 12 active sessions
5 L2TP tunnels found
```

To display detailed configuration information about specified tunnel:

```
host1#show l2tp tunnel detail 1/xyz
L2TP tunnel 1/xyz is Up with 13 active sessions
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Tunnel address
  Transport ipUdp
```

```
  Virtual router default
  Local address 192.168.1.230, peer address 172.31.1.98
  Local UDP port 1701, peer UDP port: 1701
Tunnel status
  Effective administrative state is enabled
  State is established
  Local tunnel id is 14529, peer tunnel id is 34
  Host profile is none
  Tunnel is Up for: 12 days, 8 hours, 24 minutes, 23 seconds
Sub-interfaces    total   active   failed
  Sessions        13      13       0
Statistics    packets      octets       discards   errors
  Control rx  14           683          0          0
  Control tx  41           4666         0          0
  Data rx     67900944     67900944     0          0
  Data tx     67900944     67900944     0          0
Control channel statistics
  Receive window size = 4
  Receive ZLB = 17
  Receive out-of-sequence = 0
  Receive out-of-window = 0
  Transmit window size = 4
  Transmit ZLB = 12
  Transmit queue depth = 0
  Retransmissions = 8
Tunnel operational configuration
  Peer host name is 'Juniper-POS'
  Peer vendor name is 'XYZ, Inc.'
  Peer protocol version is 1.1
  Peer firmware revision is 0x1120
  Peer bearer capabilities are digital and analog
  Peer framing capabilities are sync and async
```

Meaning Table 25 on page 164 lists the **show l2tp tunnel** command output fields.

Table 25: show l2tp tunnel Output Fields

Field Name	Field Description
Configuration	Configured status of the tunnel enabled.
Administrative state	Administrative status of the enabled tunnel: • enabled—No restrictions on creation and operation of sessions for this tunnel • disabled—Router disabled existing sessions and will not create new sessions on this tunnel • drain—Router will not create new sessions on this tunnel
SNMP traps	Whether or not the router sends traps to SNMP for operational state changes.
Tunnel address	Tunnel address information.
Transport	Method used to transfer traffic.

Table 25: show l2tp tunnel Output Fields *(continued)*

Field Name	Field Description
Virtual router	Name of the virtual router on which the tunnel is configured.
Local and peer addresses	IP addresses of the local and remote ends of the tunnel. If the router is set up to ignore address and port changes in SCCRP packets, both the transmit and receive addresses are listed for the peer.
Local and peer UDP ports	UDP ports for the local and remote ends of the tunnel. If the router is set up to accept address and port changes in SCCRP packets, both the transmit and receive UDP ports are listed for the peer.
Tunnel status	Tunnel status information.
Effective administrative state	Most restrictive of the following administrative states: E Series router, destination, and tunnel. This setting, rather than the administrative state of the tunnel, determines whether the router can create new sessions on a tunnel or whether the sessions on a tunnel are disabled or not.
State	Status of the enabled tunnel: • idle • connecting • established • disconnecting
Local and peer tunnel id	Names the router used to identify the tunnel locally and remotely.
Host profile	Name of the L2TP host profile, if it is configured. Otherwise, the label “none” is displayed to specify that a host profile is not enabled.
Tunnel is Up for	Duration for which the tunnel is operationally up, which is denoted in terms of days, hours, minutes, and seconds.
Sub-interfaces:	Sub-interface information for the enabled tunnel: • total—Number of sessions that the router has created on this tunnel • active—Number of operational sessions on the tunnel • failed—Number of requests that did not reach an operational state
Statistics	Information about the traffic sent and received.

Table 25: show l2tp tunnel Output Fields *(continued)*

Field Name	Field Description
Control channel statistics	Tunnel control channel information.
Receive window size	Number of packets that the peer can transmit without receiving an acknowledgment from the router.
Receive ZLB	Number of acknowledgments that the router has received from the peer.
Receive out-of-sequence	Number of received control packets that were out of order.
Receive out-of-window	Number of packets that arrived at the router outside the receiving window.
Transmit window size	Number of packets that the router can transmit before receiving an acknowledgment from the peer.
Transmit ZLB	Number of acknowledgments that the router has sent to the peer.
Transmit queue depth	Number of packets that the router is waiting to send to the peer, plus the number of packets for which the peer has not yet acknowledged receipt.
Tunnel operation configuration	Information received from the peer when the tunnel was created.

Related Documentation

- show l2tp tunnel on page 194

Monitoring Configured and Operational Status of All Tunnels

Purpose Display a summary of the configured and operational status of all L2TP tunnels.

Action To display a summary of the configured and operational status of all L2TP tunnels:

```
host1#show l2tp tunnel summary

Administrative status   enabled   drain   disabled
                        5         0       0
Operational status      up        down    lower-down   not-present
             5          0         0       0            0
```

Meaning Table 26 on page 167 lists the **show l2tp tunnel summary** command output fields.

Table 26: show l2tp tunnel summary Output Fields

Field Name	Field Description
Administrative status	Administrative status of all tunnels: • enabled—No restrictions on the creation and operation of sessions for this tunnel • drain—Router will not create new sessions for this tunnel • disabled—Router disabled existing sessions and will not create new sessions for this tunnel
Operational status	Operational status of all tunnels: • up—Tunnel is available • down—Tunnel is unavailable • lower-down—Tunnel is unavailable because the destination supporting it is inaccessible • not-present—Tunnel is unavailable because the hardware (such as a line module) supporting the tunnel is inaccessible

Related Documentation

- show l2tp tunnel on page 194 summary

CHAPTER 22

Monitoring L2TP Dial-Out Settings

Monitoring Chassis-wide Configuration for L2TP Dial-out

Purpose To display the chassis-wide configuration, operational state, and statistics for L2TP dial-out.

This command displays aspects of the dial-out state machine and details about the dial-out routes themselves. This section presents sample output. The actual output on your router may differ significantly.

Action To display chassis-wide configuration, operational state, and statistics for L2TP dial-out:

```
host1#show l2tp dial-out
Operational status: inService
Connecting timer value: 30 seconds
Dormant timer value: 300 seconds
```

To display detailed chassis-wide configuration information:

```
host1#show l2tp dial-out detail
    Dial-out Chassis Configuration and Operational Status
      Chassis operational status :   inService
      Dormant timeout            :   30 seconds
      Connecting timeout         :   30 seconds

Dial-out Chassis Statistics
  Current sessions:                              0
  Maximum sessions:                              0
  Current sessions in the process of connecting:   0
  Maximum sessions connecting at one time:         0
  Current sessions pending:                      0
  Maximum sessions pending:                      0
  Current targets inhibited:                     0
  Maximum targets inhibited:                     0
  Authentication grant for nonexistent session:    0
  Authentication deny for nonexistent session:     0

Dial-out Virtual router statistics
  Virtual routers active:                     0
```

```
  Virtual routers created:                        0
  Virtual routers removed:                        0
  Virtual routers in init-pending state:          0
  Virtual routers in init-failed state:           0
  Virtual routers in down state:                  0
  Virtual routers in in-service state:            0
  IP Discarded trigger frames:                    0
  Trigger frames received for unknown route:      0
  Sessions in dormant state:                      0
  Sessions in pending state:                      0
  Sessions in authenticating state:               0
  Sessions in connecting state:                   0
  Sessions in in-service state:                   0
  Sessions in inhibited state:                    0
  Sessions in post-inhibited state:               0
  Sessions in failed state:                       0

Dial-out target statistics
  Targets active:                                 0
  Targets created:                                0
  Targets removed:                                0
  Targets in down state:                          0
  Targets in inhibited state:                     0
  Targets in in-service state:                    0
  Triggers discarded:                             0
Dial-out session statistics
  Sessions active:                                0
  Sessions created:                               0
  Sessions removed:                               0
  Sessions reset:                                 0
  Triggers received:                              0
  Triggers enqueued:                              0
  Triggers discarded:                             0
  Triggers forwarded:                             0
  Triggers max enqueued:                          0
  Authentication requests:                        0
  No resources for authentication:                0
  Authentication grants:                          0
  Authentication Denies:                          0
  Dial-outs requested:                            0
  Dial-outs rejected:                             0
  Dial-outs established:                          0
  Dial-outs timed out:                            0
  Dial-outs torn down:                            0
```

To display summary information for chassis-wide configuration:

```
host1#show l2tp dial-out summary
      Virtual routers in init pending state :             0
      Virtual routers in init failed state  :             0
      Virtual routers in down state         :             0
      Virtual routers in inService state    :             0
      Targets in down state                 :             0
      Targets in inhibited state            :             0
      Targets in inService state            :             0
      Sessions in dormant state             :             0
      Sessions in pending state             :             0
      Sessions in authenticating state      :             0
      Sessions in connecting state          :             0
      Sessions in inService state           :             0
      Sessions in inhibited state           :             0
```

```
Sessions in postInhibited state       :              0
Sessions in failed state              :              0
```

To display information about the operational or administrative state:

```
host1#show l2tp dial-out state inService
```

Meaning Table 27 on page 171 lists the **show l2tp dial-out** command output fields.

Table 27: show l2tp dial-out Output Fields

Field Name	Field Description
Operational status	Current operational status of the chassis
Connecting timer value	Configuration of the connecting timeout
Dormant timer value	Configuration of the dormant timeout
Dial-out Chassis Statistics	Statistics at the chassis level
Current sessions	Total number of session currently active on the chassis
Maximum sessions	Highest value of current sessions recorded on the chassis since the last router restart
Current sessions in the process of connecting	Sessions currently in the connecting state
Maximum sessions connecting at one time	Highest number of sessions recorded on the chassis at the same time since the last router restart
Current sessions pending	Sessions in the pending state
Maximum sessions pending	Highest number of sessions recorded in the pending state since the last router restart
Current targets inhibited	Targets currently in the inhibited state
Maximum targets inhibited	Highest value of targets recorded in the inhibited state since the last router restart
Authentication grant for nonexistent session	Number of authentication requests granted to nonexistent sessions
Authentication deny for nonexistent session	Number of authentication requests denied to nonexistent sessions
Dial-out Virtual router statistics	Statistics at the virtual router level
Virtual routers active	VRs in use by the state machine
Virtual routers created	VRs that have been used by the state machine

Table 27: show l2tp dial-out Output Fields *(continued)*

Field Name	Field Description
Virtual routers removed	VRs no longer used by the state machine
Virtual routers in init-pending state	VRs in the initializationPending state
Virtual routers in init-failed state	VRs in the initializationFailed state
Virtual routers in down state	VRs in the down state
Virtual routers in in-service state	VRs in the inService state
IP Discarded trigger frames	Trigger frames that IP discarded
Trigger frames received for unknown route	Trigger frames received for an unknown route
Sessions in dormant state	Sessions on the VR that are in the dormant state
Sessions in pending state	Sessions on the VR that are in the pending state
Sessions in authenticating state	Sessions on the VR that are in the authenticating state
Sessions in connecting state	Sessions on the VR that are in the connecting state
Sessions in in-service state	Sessions on the VR that are in the inService state
Sessions in inhibited state	Sessions on the VR that are in the inhibited state
Sessions in post-inhibited state	Sessions on the VR that are in the postInhibited state
Sessions in failed state	Sessions on the VR that are in the failed state
Dial-out target statistics	Statistics at the route target level
Targets active	Current active targets
Targets created	All targets created
Targets removed	Targets deleted
Targets in down state	Targets in the down state
Targets in inhibited state	Targets in the inhibited state
Targets in in-service state	Targets in the inService state
Triggers discarded	Trigger packets discarded

Table 27: show l2tp dial-out Output Fields *(continued)*

Field Name	Field Description
Dial-out session statistics	Statistics at the session level
Sessions active	Currently active sessions
Sessions created	All sessions created
Sessions removed	Sessions deleted
Sessions reset	Sessions reset using the **l2tp dial-out session reset** command
Triggers received	Triggers received for dial-out sessions
Triggers enqueued	Triggers that have been put into the queue
Triggers discarded	Trigger packets discarded
Triggers forwarded	Trigger packets forwarded
Triggers max enqueued	Maximum number of triggers that have been enqueued simultaneously since the last router reset
Authentication requests	Authentication requests received
No resources for authentication	Authentication requests not processed because of insufficient resources
Authentication grants	Authentication requests granted
Authentication Denies	Authentication requests denied
Dial-outs requested	Outgoing calls requested for sessions
Dial-outs rejected	Outgoing call requests that were rejected
Dial-outs established	Successful outgoing calls before the connecting timer expired
Dial-outs timed out	Number of times the connecting timer expired
Dial-outs torn down	Successful outgoing calls that were terminated

Related Documentation

- L2TP Dial-Out Operational States on page 28
- show l2tp dial-out on page 188
- show l2tp dial-out virtual-router on page 191

Monitoring Dial-out Targets within the Current VR Context

Purpose Display configured dial-out targets within the current virtual router context.

This command displays aspects of the dial-out state machine and details about the dial-out routes themselves. This section presents sample output. The actual output on your router may differ significantly.

Action To display general information for all targets within the virtual router:

```
host1:dialout#show l2tp dial-out target
Target          Status      Active Sessions
------          ------      ---------------
10.10.1.1/16    up          14
10.1.1.0/24     up          10
```

To display detailed information about a particular target, specify the target IP address and mask:

```
host1:dialout#show l2tp dial-out target 10.1.1.0/24
Target 10.1.1.0/24
Operational status: up
Active sessions: 10
Total triggers: 127
Failed sessions: 2
Connected sessions: 8
```

To display aggregate counts for targets in each of the possible operational and administrative states:

```
host1:dialout#show l2tp dial-out target summary
```

To display detailed configuration, state, and statistics:

```
host1:dialout#show l2tp dial-out target detail
```

To display information about the operational or administrative state:

```
host1:dialout#show l2tp dial-out target state inService
```

To displays dial-out information across all virtual routers:

```
host1:dialout#show l2tp dial-out target allVirtualRouters
```

NOTE: The level of a user's permission determines the use of the **allVirtualRouters** option. For example, if you have permission to view only the current virtual router, then that is all that is displayed when you enter a command.

Meaning Table 28 on page 175 lists the **show l2tp dial-out target** command output fields.

Table 28: show l2tp dial-out target Output Fields

Field Name	Field Description
Target	Address of the target
Status	Status of the connection to the target
Active Sessions	Currently active session to the target
Total triggers	Trigger packets received for the target
Failed sessions	Sessions that are currently in the failed state
Connected sessions	Sessions that are currently in the connected state

Related Documentation

- L2TP Dial-Out Operational States on page 28
- show l2tp dial-out target on page 190

Monitoring Operational Status within the Current VR Context

Purpose Display dial-out state machine operational status and statistics within the current VR context.

This command displays aspects of the dial-out state machine and details about the dial-out routes themselves. This section presents sample output. The actual output on your router may differ significantly.

Action To display dial-out state machine operational status and statistics within the current VR context:

```
host1#show l2tp dial-out virtual-router
Dial-out Virtual Router Configuration and Operational Status
Virtual router host1:
Virtual router operational status: inService
Maximum trigger buffers per session: 0
```

To display aggregate counts for dial-out state machines in each of the possible operational and administrative states:

```
host1:dialout#show l2tp dial-out virtual-router summary
```

To display detailed configuration, state, and statistics:

```
host1:dialout#show l2tp dial-out virtual-router detail
```

To display information about the operational or administrative state:

```
host1:dialout#show l2tp dial-out virtual-router state down
```

To displays dial-out information across all virtual routers:

```
host1:dialout#show l2tp dial-out virtual-router allVirtualRouters
```

NOTE: The level of a user's permission determines the use of the **allVirtualRouters** option. For example, if you have permission to view only the current virtual router, then that is all that is displayed when you enter a command.

Meaning Table 29 on page 176 lists the **show l2tp dial-out virtual-router** command output fields.

Table 29: show l2tp dial-out virtual-router Output Fields

Field Name	Field Description
Virtual router	Name of VR
Virtual router operational status	Operational status of the VR
Maximum trigger buffers per session	Maximum number of trigger packets held in buffer while the dial-out session is being established

Related Documentation

- L2TP Dial-Out Operational States on page 28
- show l2tp dial-out virtual-router on page 191

Monitoring Status of Dial-out Sessions

Purpose Display the status of dial-out sessions.

This command displays aspects of the dial-out state machine and details about the dial-out routes themselves. This section presents sample output. The actual output on your router may differ significantly.

Action To display all sessions within the current virtual router context:

```
host1#show l2tp dial-out session
Session          Status
---------        ---------
10.10.1.1        connected
10.10.2.1         dormant
```

To display detailed information about a particular session, specify the trigger IP address for the session:

```
host1#show l2tp dial-out session 10.1.1.1
Session 10.1.1.1
Operational status: dormant
```

To display aggregate counts for dial-out sessions in each of the possible operational and administrative states:

```
host1#show l2tp dial-out session summary
```

To display detailed configuration, state, and statistics:

```
host1#show l2tp dial-out session detail
```

To display information about the operational or administrative state:

```
host1#show l2tp dial-out session state connecting
```

To display dial-out information across all virtual routers

```
host1#show l2tp dial-out session allVirtualRouters
```

NOTE: The level of a user's permission determines the use of the **allVirtualRouters** option. For example, if you have permission to view only the current virtual router, then that is all that is displayed when you enter a command.

Meaning Table 30 on page 177 lists the **show l2tp dial-out session** command output fields.

Table 30: show l2tp dial-out session Output Fields

Field Name	Field Description
Session	IP address of the session
Status	Current status of the session
Operational status	Current operational status of session

Related Documentation

- L2TP Dial-Out Operational States on page 28
- **show l2tp dial-out session on page 189**

CHAPTER 23

Monitoring Commands

show aaa domain-map

Syntax show aaa domain-map [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the mapping between user domains and virtual routers. The display includes a tunnel group if one is assigned to the domain map.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show aaa tunnel-group

Syntax show aaa tunnel-group [*tunnelGroupName*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays currently configured tunnel groups.

Options
- *tunnelGroupName*—Name of the tunnel group
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show aaa tunnel-parameters

Syntax show aaa tunnel-parameters [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays default tunnel parameters that are configured for tunnel definitions.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp

Syntax show l2tp [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about the L2TP configuration on the router.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp destination

Syntax show l2tp destination [detail] [*destinationName* |
[virtual-router *vrName*] ip *ipAddress*] [*filter*]

show l2tp destination summary [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays information about selected L2TP destinations.

Options

- detail—Provides complete information about the specified destinations, including destination profiles
- *destinationName*—Name the router assigns to the peer at the other end of the tunnel
- *vrName*—Name of the virtual router on which the destination exists
- *ipAddress*—IP address of the peer at the other end of the tunnel
- summary—Displays a summary of destination profile configuration
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp destination lockout

Syntax show l2tp destination lockout [*filter*]

Release Information Command introduced in JunosE Release 7.2.0.

Description Displays information about the L2TP destinations that are currently unavailable because they are in the lockout state.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp destination profile

Syntax show l2tp destination profile [*profileName*] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays destination profile configuration.

Options
- *profileName*—Name of a profile
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp received-disconnect-cause-summary

Syntax show l2tp received-disconnect-cause-summary [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays aggregate summary statistics for all information received by an LAC from an LNS about the cause of an L2TP session disconnection. The LAC receives this information from the LNS by means of a PPP Disconnect Cause Code attribute value pair (AVP) included in an L2TP Call-Disconnect-Notify (CDN) message.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp dial-out

Syntax show l2tp dial-out [[detail] [state *operState*] | summary] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the chassis-wide configuration, operational state, and statistics for L2TP dial-out.

Options

- detail—Displays configuration, states, and statistics
- *operState*—One of the following operational states:
  - inService
  - initIncomplete
  - restricted
- summary—Displays aggregate counts for virtual routers, targets, and sessions in each of the possible operational and administrative states
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp dial-out session

Syntax show l2tp dial-out session [*triggerIpAddress* | allVirtualRouters] [detail] [state *operState*] [*filter*]

To display summary information:

show l2tp dial-out session summary [allVirtualRouters] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the status of L2TP dial-out sessions.

Options

- *triggerIpAddress*—Trigger IP address for the session that you want to display
- allVirtualRouters—Displays dial-out information for all virtual routers
- detail—Displays configuration, state, and statistics
- *operState*—One of the following operational states:
  - authenticating
  - connecting
  - dormant
  - failed
  - inService
  - inhibited
  - pending
  - postInhibited
- *filter*—See *Filtering show Commands*
- summary—Displays aggregate counts for dial-out sessions in each of the possible operational and administrative states

Mode Privileged Exec

show l2tp dial-out target

Syntax show l2tp dial-out target [*targetIpAddress targetIpAddressMask* | allVirtualRouters] [detail] [state *operState*] [*filter*]

To display summary information:

show l2tp dial-out target summary [allVirtualRouters] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays configured dial-out targets within the current virtual router context.

Options

- *targetIpAddress*—Trigger IP address for the target that you want to display
- *targetIpAddressMask*—Mask for the trigger IP address
- allVirtualRouters—Displays dial-out information for all virtual routers
- detail—Displays configuration, state, and statistics
- *operState*—One of the following operational states:
  - down
  - inService
  - inhibited
- *filter*—See *Filtering show Commands*
- summary—Displays aggregate counts for targets in each of the possible operational and administrative states

Mode Privileged Exec

show l2tp dial-out virtual-router

Syntax show l2tp dial-out virtual-router [allVirtualRouters] [detail] [state *operState*] [*filter*]

To display summary information:

show l2tp dial-out virtual-router summary [allVirtualRouters] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays dial-out state machine operational status and statistics within the current virtual router context.

Options

- allVirtualRouters—Displays dial-out information across all virtual routers
- detail—Displays configuration, state, and statistics
- *operState*—One of the following operational states:
  - down
  - inService
  - initFailed
  - initPending
- *filter*—See *Filtering show Commands*
- summary—Displays aggregate counts for dial-out state machines in each of the possible operational and administrative states

Mode Privileged Exec

show l2tp session

Syntax show l2tp session [detail] [state { *adminState* | *ifOperStatus* }]
[*l2tpName* | [virtual-router *vrName*] ip *ipAddress* [*l2tpNameNoDest*]] [*filter*]

To display summary information:

show l2tp session summary [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays detailed information about selected L2TP sessions or summary information for all L2TP sessions.

Options

- detail—Provides complete information about the specified sessions
- state—Restricts display to sessions in a specific state
- *adminState*—Effective administrative state
- *ifOperStatus*—Operational state
- *l2tpName*—Session name
- *vrName*—Name of the virtual router on which the session exists
- *ipAddress*—IP address
- *l2tpNameNoDest*—Name of the session
- *filter*—See *Filtering show Commands*
- summary—Displays the configured and operational status of all L2TP sessions

Mode Privileged Exec

show l2tp switch-profile

Syntax show l2tp switch-profile [*profileName*] [*filter*]

Release Information Command introduced in JunosE Release 7.2.0.

Description Displays the names of all L2TP tunnel switch profiles currently configured on the router, or displays detailed information about a particular L2TP tunnel switch profile.

Options
- *profileName*—Name of the tunnel switch profile; a string of up to 64 alphanumeric characters
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

show l2tp tunnel

Syntax show l2tp tunnel [detail] [state { *adminState* | *ifOperStatus* | failover-resync *failoverResyncMode* }]
[*l2tpName* | [virtual-router *vrName*] ip *ipAddress* [*l2tpNameNoDest*]] [*filter*]

To display summary information:

show l2tp tunnel summary [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
failover-resync keyword and *failoverResyncMode* variable added in JunosE Release 9.0.0.

Description Displays detailed information about the configured and operational status of selected L2TP tunnels or summary information for all L2TP tunnels.

Options

- detail—Provides complete information about the specified sessions, including the L2TP host profile name
- *adminState*—Displays information about tunnels only with the specified effective administrative state
  - enabled—Effective administrative state is disabled
  - disabled—Effective administrative state is enabled
  - drain—Effective administrative state is drain
- *ifOperStatus*—Displays information about tunnels only with the specified operational state
  - up—Operational state is up
  - down—Operational state is down
  - lower-down— Operational state is lower down
  - not-present—Operational state is not-present
- *failoverResyncMode*—Displays information about tunnels that use the specified failover resynchronization mode:
  - disable—Peer failover resynchronization is disabled
  - failover-protocol—Uses the L2TP failover protocol method
  - failover-protocol-fallback-to-silent-failover—Uses the L2TP failover protocol method; however, if the peer does not support this method, the silent failover method is used
  - not-configured—Uses the global failover method because peer failover resynchronization is not configured for L2TP host profiles and AAA domain map tunnels
  - silent-failover—Uses the L2TP silent failover method
- *l2tpName*—Tunnel name

- *vrName*—Name of the virtual router on which the tunnel exists
- *ipAddress*—IP address
- *l2tpNameNoDest*—Tunnel name
- *filter*—See *Filtering show Commands*
- summary—Displays the configured and operational status of all L2TP tunnels

Mode Privileged Exec

PART 4

Index

Index

S

T

U

V